Bureau de la vérificatrice générale de l'Ontario

# Audit de l'optimisation des ressources :

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

*Novembre 2022*

Ministère des Services au public et aux entreprises (MSPE)

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

## 1.0 Résumé

La fonction publique de l'Ontario (FPO) a recours à un vaste éventail de systèmes de technologie de l'information (TI) pour offrir des programmes et des services gouvernementaux, depuis la délivrance de cartes Santé et de permis de conduire jusqu'à la prestation de programmes de soutien aux familles et de subventions pour la COVID-19. Les systèmes de TI sont devenus cruciaux pour la population ontarienne. En 1998, le gouvernement de l'Ontario a mis sur pied le Bureau du directeur général de l'information pour la fonction publique (le Bureau du DGIFP) pour fournir un soutien en TI à tous ses ministères provinciaux ainsi qu'au Bureau du Conseil des ministres et au Cabinet du premier ministre.

Le Bureau du DGIFP est directement responsable des besoins en TI qui existent dans l'ensemble de la FPO. Par exemple, le Bureau du DGIFP établit et tient à jour la planification stratégique, les politiques, les normes et les pratiques exemplaires en matière de TI, comme les normes de sécurité de l'information, de développement des applications et de gestion des bases de données. Au nom des ministères, il achète et entretient du matériel comme des ordinateurs portables et des téléphones mobiles pour tous les employés de la FPO, et il est responsable de protéger le réseau global de TI de la FPO contre les cyberattaques. De plus, le Bureau du DGIFP gère deux Centres des données, situés à Guelph et à Kingston, qui hébergent les serveurs et les bases de données associées à 1 200 systèmes de TI qui stockent les données des Ontariens.

Huit « groupements » de services de TI répondent directement aux besoins des ministères en matière de TI parce qu'ils sont chargés de fournir des services et du soutien de TI propres à un groupement particulier de ministères. Par exemple, l'un des groupements des services de TI est le groupement des services de santé. Il rassemble le ministère de la Santé et le ministère des Soins de longue durée et exploite de nombreux systèmes de TI propres au secteur des soins de santé, comme le Système d'inscription des clients, pour stocker les données sur les patients et leurs coordonnées. Les huit groupements de TI sont gérés par les ministères et relèvent des sous-ministres. Le Bureau du DGIFP fournit des services et offre des consultations à ces employés du groupement, qui, à leur tour, gèrent les systèmes de TI utilisés par le public ontarien et prennent des décisions à ce sujet.
Le Bureau du DGIFP relève du ministère des Services au public et aux entreprises (le Ministère) et a pour mandat de veiller à ce que les services de TI du gouvernement provincial soient fournis de façon efficace et efficiente. Notre audit a révélé que l'une des conséquences de la structure hiérarchique – selon laquelle les groupements de TI relèvent de leurs sous-ministres respectifs et non du Bureau du DGIFP – est que ce dernier n'a pas de surveillance, de reddition de comptes ni d'autorité pour les opérations courantes des TI et la prise de décisions dans les huit groupements de TI. Sans une telle surveillance, le Bureau du DGIFP est incapable de s'acquitter de son mandat et de s'assurer

que les services de TI comme l'approvisionnement, le rendement des fournisseurs et la cybersécurité sont bel et bien fournis efficacement et dans le respect de l'économie.

Nous avons déterminé que les pratiques de cybersécurité de la FPO devaient être améliorées. Les données personnelles et sensibles des Ontariens stockées dans les systèmes informatiques que nous avons examinés n'étaient pas protégées au moyen de contrôles de cybersécurité comme le chiffrement. Nous avons examiné les contrôles liés aux évaluations de cybersécurité. En raison de la nature de la cybersécurité et afin de réduire au minimum le risque d'exposition pour la fonction publique de l'Ontario, nous avons fourni des détails pertinents de nos constatations et recommandations directement au Bureau du DGIFP. Le Bureau du DGIFP a convenu du bien-fondé de la recommandation et s'est engagé à protéger les données confiées au gouvernement par la population et les entreprises de l'Ontario. Nous avons également constaté que la moitié des systèmes de TI essentiels à l'exécution continue et fiable des programmes gouvernementaux ne comportent pas de plan de reprise après sinistre en cas de panne importante ou de catastrophe.

Nous avons également constaté que le centre de traitement de l'information le mieux coté de l'Ontario, utilisé par le Bureau du DGIFP pour héberger des serveurs et des bases de données pour l'ensemble des 1 200 systèmes de TI de la FPO, était considérablement sous-utilisé depuis son ouverture il y a 10 ans, et que son utilisation a même diminué au cours des 5 dernières années. Bien que le centre de données ait été construit en mars 2011 dans le but de fournir des services à la FPO, une analyse de rentabilisation a été soumise au Secrétariat du Conseil du Trésor en 2012 dans le but de tirer parti du centre de données à des fins d'utilisation par le secteur parapublic à l'extérieur de la FPO. Malgré cette capacité, les organismes du secteur parapublic et de la Couronne n'en font qu'une utilisation minimale à l'heure actuelle. En raison de l'utilisation limitée du centre, le Bureau du DGIFP qui est le gardien du centre de traitement de l'information a engagé des dépenses de fonctionnement supplémentaires d'environ 31 millions de dollars (au cours des cinq dernières années) pour l'électricité, le refroidissement, l'entretien et la sécurité physique de l'espace inoccupé. Ce coût aurait pu être compensé par l'occupation de l'espace non utilisé par d'autres entités gouvernementales, comme les organismes de la Couronne et le secteur parapublic, qui en partageraient les coûts.

Voici quelques-unes des constatations dignes de mention de l'audit que nous avons effectué :

## Gouvernance

- **Le Bureau du DGIFP exerce une faible surveillance des activités de TI dans les huit groupements de TI.** Le Bureau du DGIFP n'est pas en mesure de s'acquitter de son mandat, qui consiste à s'assurer que les services de TI du gouvernement sont gérés et fournis efficacement, puisqu'il n'est pas responsable des opérations de TI exécutées par les huit groupements de TI. Les groupements relèvent de leurs sous-ministres respectifs et non du 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 (de moins de 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 de TI des groupements.
- **Le Bureau du DGIFP n'a pas cerné les risques liés aux TI pour l'organisme et les stratégies d'atténuation ayant une incidence sur les activités de la FPO.** À l'heure actuelle, les risques de TI ne sont pas cernés au sein du Bureau du DGIFP et celui-ci n'a pas de stratégie globale permettant à la FPO d'établir les risques de TI et de mettre en œuvre des stratégies d'atténuation et de correction. Nous avons remarqué que le Bureau du DGIFP s'en remettait aux ministères et aux groupements pour déterminer les éléments de risque de TI qui ont une incidence sur un ministère ou un

groupement en particulier. Après avoir examiné les risques cernés, nous avons constaté que le Bureau du DGIFP n'avait pas relevé de risques majeurs en matière de TI qui auraient une incidence sur la FPO ni de risques couramment cernés par les pratiques exemplaires de l'industrie.

- **Le centre de traitement de l'information principal de l'Ontario est très sous-utilisé.** Le centre de traitement de l'information a obtenu une cote de niveau IV, la cote la plus élevée disponible pour un centre de traitement de l'information indiquant que les systèmes de TI sont en mesure de résister à tout type de défaillance. Au moment de notre audit, le Centre des données de Guelph servait à 30 % de sa capacité, à un coût annuel total de 9 millions de dollars. Deux facteurs principaux expliquent cette faible utilisation :
  - La tarification standard pour l'utilisation du centre de traitement de l'information s'établit à 75 $ le pied carré (soit 1,33 $/kWh après conversion en électricité aux fins de comparaison), soit plus du double par rapport aux autres exploitants privés de centres de traitement de l'information de niveau IV qui facturent 0,59 $/kWh dans d'autres pays comme les États-Unis, le Royaume-Uni et l'Australie.
  - L'absence d'une stratégie de marketing pour promouvoir le centre de traitement de l'information à l'extérieur de la FPO auprès des organismes de la Couronne et du secteur parapublic.

## Reprise après sinistre

- **Près de la moitié des systèmes de TI essentiels de la FPO n'ont pas de plan de reprise après sinistre.** Nous avons constaté que près de la moitié (44 %) de tous les systèmes de TI essentiels, qui sont essentiels à la continuité des services gouvernementaux comme la santé, l'éducation et les permis de conduire, n'ont pas de plan de reprise après sinistre. De tels plans décrivent des procédures détaillées pour récupérer et restaurer un système de TI après un sinistre, comme une panne prolongée d'Internet ou une cyberattaque majeure. Plus particulièrement, nous avons remarqué que le Bureau du DGIFP ne dispose pas d'un fournisseur de réseau secondaire redondant pour certaines de ses activités essentielles, comme les 44 centres de contact, sur lequel il pourrait compter en cas de panne pour maintenir la fonctionnalité de ses systèmes de TI essentiels. Par conséquent, la panne de Rogers Communications survenue à l'échelle nationale le 8 juillet 2022 a eu des répercussions sur la FPO, qui n'a pas été en mesure de fournir des services aux Ontariens par l'entremise de centres de contact comme Service Ontario, les cliniques de vaccination contre la COVID-19 et les sites Web des paiements d'aide sociale.

## Cybersécurité

- **Les données personnelles et sensibles ne sont pas toujours protégées par chiffrement conformément à la norme de sécurité du Bureau du DGIFP.** Dans un échantillon de cinq systèmes de TI clés utilisés par le ministère de la Santé, le ministère du Solliciteur général, le ministère de la Sécurité Communautaire et des Services correctionnels et le ministère des Services au public et aux entreprises, nous avons découvert que des renseignements personnels et sensibles n'étaient chiffrés dans aucun d'entre eux, alors qu'ils devraient l'être conformément à la norme de sécurité.
- **Il n'existe aucune surveillance en matière de cybersécurité des données des Ontariens stockées par des fournisseurs de TI.** Le Bureau du DGIFP ne supervise pas les risques liés à la cybersécurité pour 140 systèmes de TI de la FPO gérés par des fournisseurs externes de la FPO, car il n'obtient ni n'examine les rapports d'assurance de tiers.
- **La formation sur la sensibilisation à la cybersécurité dans la FPO peut être renforcée.** Le Bureau du DGIFP est responsable de l'élaboration et de la mise en œuvre de la

formation sur la cybersécurité à l'intention du personnel de la FPO. Nous avons constaté que seulement 11 000 des 40 000 employés de la FPO ont suivi le cours obligatoire de sensibilisation à la cybersécurité en 2021. Bien que les gestionnaires des employés soient responsables de veiller à ce que cette formation soit suivie, le Bureau du DGIFP ne fait pas le suivi du cours et ne s'assure pas que tout le personnel y assiste. De plus, la formation de sensibilisation à la cybersécurité n'est pas requise pour environ 7 000 employés contractuels, et n'est pas non plus offerte sur une base annuelle aux employés de la FPO, même si elle est considérée comme une pratique exemplaire.

### Obtention de services de consultants

- **La diligence raisonnable est insuffisante dans le contexte de l'embauche de consultants en TI.** Avant d'embaucher du personnel contractuel, le Bureau du DGIFP n'évalue pas s'il dispose déjà des ressources internes pour effectuer le travail, ou s'il devrait embaucher un employé permanent à temps plein ou un consultant. D'après notre analyse, le Bureau du DGIFP a versé aux consultants le double du salaire qu'il aurait versé à du personnel à temps plein pour les mêmes postes. De plus, du 1er avril 2021 au 31 mai 2022, quelque 25 consultants sur un total de 244 ont été rémunérés en moyenne 86 $ de plus que le taux quotidien recommandé par le Secrétariat du Conseil du Trésor. Le trop-payé le plus élevé était de 232 $ au-dessus du taux quotidien établi, sans justification.

### Résolution des incidents de TI

- **Les cibles de résolution des incidents de TI ne sont pas atteintes.** En 2016, le Bureau du DGIFP s'est fixé une cible de conformité de 90 % pour la résolution des incidents de TI, comme établi dans les ententes sur les niveaux de service. Cette cible n'a pas été réévaluée depuis. Les données du DGIFP indiquent une conformité moyenne de 95 % pour tous les incidents de TI au cours des cinq dernières années. Lorsque nous avons recalculé le taux de conformité à la résolution, nous avons constaté que le taux moyen de résolution était de 85 %. Cet écart de 10 % est attribuable au fait que le Bureau du DGIFP calcule le taux de conformité en utilisant le temps écoulé, soit le temps consacré par le technicien pour résoudre le billet d'incident, alors que pour notre calcul, nous avons comparé le temps écoulé entre le moment de la création du billet d'incident et de la fermeture du billet. Nous avons également constaté que le taux de conformité des incidents de TI ayant les répercussions les plus importantes (« critiques ») était de 66 %.

## Conclusion globale

Notre audit a permis de conclure que le Bureau du directeur général de l'information pour la fonction publique (le Bureau du DGIFP) de l'Ontario n'exerce pas une surveillance approfondie des opérations de technologie de l'information (TI) et de la prestation des services de TI au sein de la fonction publique de l'Ontario (FPO). En raison de la structure hiérarchique actuelle – selon laquelle les ministères « groupés » relèvent de leurs sous-ministres respectifs plutôt que du DGIFP – le DGIFP ignore souvent les décisions clés en matière d'approvisionnement en TI et de sécurité des données et ne peut ni surveiller ni mesurer le rendement de la plupart des systèmes de TI essentiels utilisés par la FPO. Bien que le Bureau du DGIFP assume la responsabilité globale de ces systèmes de TI conformément à son mandat, la structure hiérarchique actuelle constitue un obstacle important à la réalisation de son mandat, à savoir optimiser les ressources de l'infrastructure technologique qui alimente l'ensemble du gouvernement et assurer la protection des renseignements personnels, la sécurité, la disponibilité et l'intégrité de l'information, des opérations, des réseaux et des systèmes essentiels du gouvernement.

De plus, nous avons constaté que le Centre des données de Guelph de la FPO, qui a la cote la plus élevée au monde et qui est utilisé par les ministères et

plusieurs autres organismes gouvernementaux pour héberger leurs systèmes de TI, était considérablement sous-utilisé depuis son entrée en service il y a 10 ans. Bien que le centre de données ait été construit en mars 2011 dans le but de fournir des services à la FPO, une analyse de rentabilisation a été soumise au Secrétariat du Conseil du Trésor en 2012 dans le but de tirer parti du centre de données à des fins d'utilisation par le secteur parapublic à l'extérieur de la FPO. Malgré cette capacité, les organismes du secteur parapublic et de la Couronne n'en font qu'une utilisation minimale à l'heure actuelle. L'utilisation a même diminué au cours des cinq dernières années, période pendant laquelle 31 millions de dollars supplémentaires ont été consacrés directement à l'électricité, au refroidissement, à l'entretien et à la sécurité physique de l'espace inoccupé. L'une des raisons de la faible utilisation du centre de traitement de l'information est son coût élevé pour les clients, qui représente plus du double du montant facturé par les autres centres de traitement de l'information de niveau IV. De plus, le Bureau du DGIFP n'a pas de stratégie de sensibilisation pour intégrer d'autres entités gouvernementales.

Nous avons également constaté que le Bureau du DGIFP ne dispose pas de plan de reprise après sinistre pour près de la moitié des systèmes de TI essentiels de la FPO. Les plans de reprise après sinistre appuient le fonctionnement continu et fiable des programmes gouvernementaux si un événement imprévu affecte ses systèmes de TI. De plus, le Bureau du DGIFP n'a pas élaboré de stratégie globale de reprise après sinistre et n'a pas effectué de tests exhaustifs de reprise après sinistre pour tous les systèmes de TI essentiels de la FPO.

En ce qui concerne les renseignements personnels et sensibles des Ontariens, nous avons constaté que ces renseignements ne sont pas entièrement protégés conformément à la norme de sécurité (p. ex. par chiffrement des données). Nous avons examiné les contrôles liés aux évaluations de cybersécurité. En raison de la nature de la cybersécurité et afin de réduire au minimum le risque d'exposition pour la fonction publique de l'Ontario, nous avons fourni des détails pertinents de nos constatations et recommandations directement au Bureau du DGIFP. Le Bureau du DGIFP a convenu du bien-fondé de la recommandation et s'est engagé à protéger les données confiées au gouvernement par la population et les entreprises de l'Ontario.

Le présent rapport renferme 13 recommandations préconisant 40 mesures à prendre pour donner suite aux constatations de notre audit.

## RÉPONSE GLOBALE DU MINISTÈRE

Le ministère des Services au public et aux entreprises (le Ministère) remercie la vérificatrice générale et son équipe pour ce rapport d'optimisation des ressources du Bureau du directeur général de l'information pour la fonction publique (DGIFP).

Le Bureau du DGIFP au sein du Ministère s'engage à protéger les données confiées au gouvernement par la population et les entreprises de l'Ontario. Le Ministère utilise une approche de défense en profondeur en matière de cybersécurité, qui comprend plusieurs niveaux de contrôles de sécurité, pour cerner les faiblesses inhérentes à la cybersécurité dans les systèmes de TI de la FPO. Le Ministère reconnaît qu'il y a place à l'amélioration et s'engage à continuellement évoluer et à améliorer ses pratiques de cybersécurité actuelles. Cela passe notamment par le renforcement de la gestion du rendement des fournisseurs grâce à la centralisation de la gestion des principaux fournisseurs de TI et à une gestion et une surveillance efficaces du rendement. Au cours des dernières années, le Ministère a fait des progrès en ce qui concerne les pratiques de maturité en matière de cybersécurité. Sa prochaine stratégie de cybersécurité (2023-2026) mettra l'accent sur le renforcement de la posture de cybersécurité de la FPO, tout en habilitant le secteur parapublic et en étendant le soutien aux secteurs clés (santé, éducation).

Pour soutenir le virage numérique du gouvernement, au cours de la dernière décennie, le Ministère a regroupé 22 centres de données régionaux en 2 centres de données à Guelph et à Kingston, réduisant ainsi l'empreinte des centres

de données du gouvernement, en plus des travaux en cours pour mettre hors service le centre de données de Kingston au cours des deux prochaines années. Le gouvernement continue de réduire son empreinte en adoptant des technologies novatrices pour accroître l'efficacité opérationnelle, la fiabilité, la disponibilité et l'optimisation des ressources. Alors que le gouvernement continue d'adopter des technologies novatrices, le Ministère s'engage à respecter des principes clés pour assurer la protection, la sécurité et la protection des renseignements personnels des Ontariens. En collaboration avec ses partenaires et ceux des groupements, le Ministère intégrera la cybersécurité dès sa conception dans toutes les applications afin de renforcer leur fiabilité et leur efficience et de permettre une utilisation plus stratégique et efficace des actifs et des ressources de TI.

Le Ministère reconnaît également qu'il est possible d'en faire davantage pour s'attaquer aux risques organisationnels liés aux TI. En plus de cerner ces risques, le Ministère s'est engagé à poursuivre sa collaboration avec le Bureau du directeur général de la gestion des risques afin d'améliorer les pratiques de gestion des risques et de mieux surveiller et gérer les risques à l'échelle organisationnelle.

Le Ministère s'engage à prendre toutes les mesures nécessaires et à mettre en application les recommandations du présent rapport pour améliorer continuellement la prestation des services des systèmes de TI du gouvernement.

# 2.0 Contexte

## 2.1 Aperçu

Le mandat du Bureau du directeur général de l'information pour la fonction publique (le Bureau du DGIFP) est de veiller à ce que les systèmes de TI du gouvernement de l'Ontario soient gérés et mis en œuvre de manière efficiente et efficace. Pour ce faire, il doit appuyer tous les ministères provinciaux dans leurs initiatives et investissements en TI. Le Bureau du DGIFP est directement responsable des besoins en TI à l'échelle de la FPO, comme l'acquisition de biens, le maintien de la cybersécurité, l'élaboration de politiques et de procédures de TI, comme la sécurité de l'information, le développement des applications et les normes de gestion des bases de données, et la supervision des activités quotidiennes des deux centres de traitement de l'information de la FPO situés à Guelph et à Kingston. Les besoins en TI propres aux ministères sont traités séparément par huit « groupements » de services chargés de fournir des services de TI propres à un groupe particulier de ministères (comme il est expliqué à la **section 2.2**).

Le Bureau du DGIFP fait partie du ministère des Services au public et aux entreprises (le Ministère) et comprend quatre divisions : Services technologiques d'infrastructure (STI), Division de la cybersécurité (DCS), Prestation en matière de technologie pour la FPO (PTF) et Stratégie en matière de technologie pour la FPO (STF). La **figure 1** résume les attributions de chaque division. Au total, le Bureau du DGIFP compte environ 1 250 employés en TI. Plus de 1 000 de ces employés travaillent à la Division des STI. On trouve à l'**annexe 1** un glossaire des acronymes utilisés dans le présent rapport.

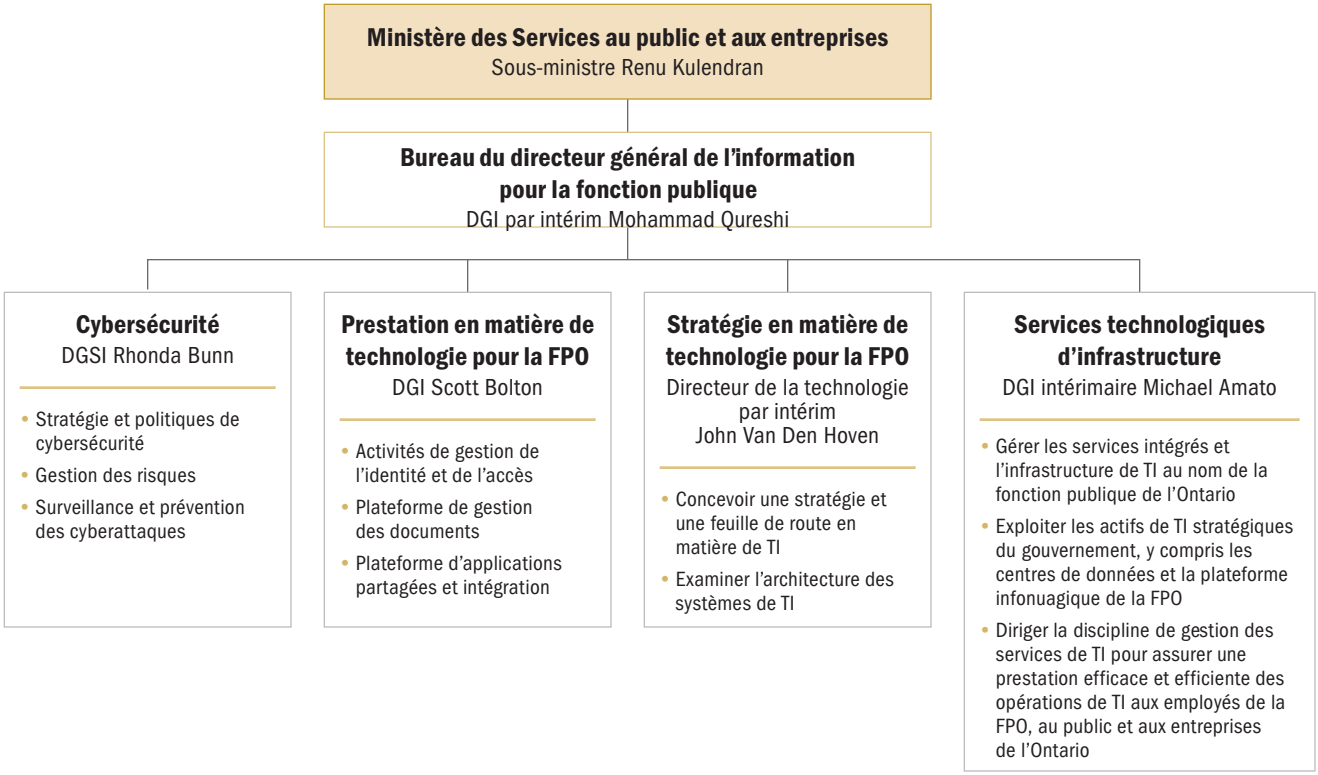
### 2.1.1 Quatre divisions intégrées du DGIFP

#### Services technologiques d'infrastructure

Les Services technologiques d'infrastructure (STI) sont chargés de fournir du matériel, comme des ordinateurs portables, des téléphones cellulaires et des imprimantes, ainsi que des applications logicielles à l'échelle de l'organisation, comme Microsoft Office, à environ 60 000 employés de la FPO dans des bureaux partout en Ontario. Les STI gèrent les activités opérationnelles quotidiennes dans leurs deux centres de traitement de l'information, qui stockent environ 1 200 systèmes de TI utilisés à l'interne par les ministères et auprès du public. Pour offrir des programmes gouvernementaux et des services essentiels aux Ontariens, le Centre de données

**Figure 1 : Divisions intégrées du Bureau du directeur général de l'information pour la fonction publique (Bureau du DGIFP)**

Préparée par le Bureau de la vérificatrice générale de l'Ontario




de Guelph doit veiller à ce que les données soient protégées et accessibles, avec le moins de perturbations possible. Il existe une ligne d'assistance téléphonique 24 heures sur 24 du Centre d'appels de service de la FPO, qui fournit un soutien technique par téléphone, à distance et en personne pour les demandes comme la réinitialisation des mots de passe et le dépannage général en matière de TI pour tous les employés de la FPO.

Les STI fournissent au personnel de la FPO et à ses deux centres de traitement de l'information les biens de TI appropriés, comme les ordinateurs portables, les ordinateurs de bureau, les périphériques et les serveurs. Il incombe aux groupements de TI de demander des biens, comme des ordinateurs portables, des imprimantes et des appareils téléphoniques, au nom des ministères qui font partie du groupement. En janvier 2022, les STI géraient plus de 90 000 ordinateurs portables et de bureau, 45 000 appareils mobiles et 10 000 serveurs pour le compte des ministères. Les STI gèrent trois catégories de biens (voir la **section 2.5**).

De plus, les STI fournissent l'infrastructure qui soutient les systèmes de TI essentiels des ministères et des organismes.

## Cybersécurité

La Division de la cybersécurité du Bureau du DGIFP, qui est responsable de la définition des exigences de cybersécurité de la FPO au moyen de politiques et de procédures, effectue systématiquement des analyses de vulnérabilité des systèmes de TI essentiels pour repérer les vulnérabilités éventuelles. En outre, la Division de la cybersécurité recommande des mesures de protection et des contrôles compensatoires au moyen d'évaluations ponctuelles de la cybersécurité, comme des tests de pénétration et des évaluations des menaces et des risques. La mise en œuvre et l'opérationnalisation de ces recommandations relèvent des propriétaires des réseaux. La Division de la cybersécurité est également responsable des activités

liées à la sécurité de l'information pour tous les ministères et groupements de la FPO. La Division met l'accent sur une meilleure sensibilisation et éducation en matière de cybersécurité chez le personnel du gouvernement de l'Ontario et sur la lutte contre les cyberrisques élevés. Elle fournit également des services tels que la surveillance des cyberattaques, l'évaluation des menaces et des risques, la prestation de conseils en matière de sécurité, l'examen de l'architecture des réseaux de TI et la prestation de conseils sur les achats liés à la sécurité. La Division applique diverses politiques, normes et lignes directrices en matière de cybersécurité à l'échelle de la FPO. La Division a également établi une norme de cybersécurité pour les groupements et les ministères, qui les oblige à protéger les renseignements de nature délicate en utilisant des contrôles de sécurité comme le chiffrement.

La Division de la cybersécurité exploite également le Centre des opérations en matière de cybersécurité, accessible aux employés de la FPO 24 heures sur 24. Le Centre des opérations repère et signale les incidents, intervient en la matière, les prévient et s'occupe du filtrage Web. L'Unité de conception de solutions sécurisées de la Division de la cybersécurité fournit des conseils et des directives sur la configuration des systèmes et des solutions d'information afin de répondre aux exigences de sécurité fondées sur des évaluations de sécurité. Au sein de l'Unité de gestion des vulnérabilités de la Division de la cybersécurité, le personnel effectue des évaluations de la vulnérabilité, des tests de pénétration et des évaluations des menaces et des risques.

En 2019, le Bureau du DGIFP a mis sur pied un Centre d'excellence pour la cybersécurité, dirigé par la Division de la cybersécurité. Le Centre offre des séminaires, des ateliers et un programme en ligne de sensibilisation à la cybersécurité aux employés du secteur parapublic pour les sensibiliser davantage aux risques liés à la cybersécurité. Il mène également des campagnes mensuelles et conseille les ministères et organismes clients sur les pratiques exemplaires en matière de cybersécurité et les normes pertinentes de l'industrie. Le Centre d'excellence pour la cybersécurité est également responsable de l'élaboration et de la prestation de cours de formation et de sensibilisation en cybersécurité au moyen du système de TI LearnON, accessible à tous les employés de la FPO.

### Prestation en matière de technologie pour la FPO

La Division de la prestation en matière de technologie pour la FPO est responsable de gérer une partie importante des systèmes d'authentification gouvernementaux qui gèrent l'accès aux systèmes de TI du gouvernement. La Division gère également un système de TI de gestion des documents appelé OPSdocs, qui est largement intégré à plusieurs systèmes de TI de la FPO et qui offre des fonctions d'hébergement de documents, de recherche et de gestion des dossiers. La Division de la prestation en matière de technologie pour la FPO gère également une plateforme technologique qui héberge plusieurs systèmes de TI essentiels à la mission et fournit des services d'intégration entre les systèmes afin qu'ils puissent échanger des données et effectuer des transactions à l'appui des processus opérationnels.

### Stratégie en matière de technologie pour la FPO

La Division de la stratégie en matière de technologie pour la FPO (DSTF) a été créée récemment, soit le 1er avril 2021. Elle est chargée de concevoir et de tenir à jour des normes, politiques et procédures en matière de TI et d'élaborer une stratégie et une vision globales en TI à l'échelle de la FPO. La DSTF travaille en collaboration avec les groupements de TI et leurs ministères. La DSTF a établi une stratégie appelée feuille de route technologique et plan d'investissement qui décrit le plan d'investissement technologique, définit et priorise les technologies communes au sein de la FPO qui pourraient être utilisées par les ministères, et utilise les ressources de TI de la manière la plus efficiente possible.

La Division de la stratégie en matière de technologie pour la FPO régit la conception des projets à risque élevé ou qui coûtent deux millions de dollars ou plus. Pour ce faire, elle doit notamment présider le Conseil d'examen de l'architecture technologique

organisationnelle qui supervise la pratique de l'architecture organisationnelle de la FPO, coordonner la sécurité, la protection des renseignements personnels et l'accessibilité, et consigner les examens de la gestion.

### 2.1.2 Financement du DGIFP

En 2021-2022, les dépenses de fonctionnement totales du Bureau du DGIFP étaient de 144 millions de dollars et comportaient 9,2 millions de dollars en dépenses en capital. Il convient de souligner que les STI sont de loin la plus importante division de l'organisation. En 2021-2022, les salaires et traitements dans cette division s'élevaient à 99,8 millions de dollars.

En 2020-2021, les dépenses ont totalisé 117 millions de dollars en coûts de fonctionnement et 9,6 millions de dollars en dépenses en immobilisations.

## 2.2 Les huit groupements de TI

Bien que les 4 divisions intégrées du Bureau du DGIFP répondent aux besoins, aux initiatives et aux projets à l'échelle de la FPO, comme les services de courriel et de téléphone, 8 « groupements » de TI (totalisant environ 2 400 employés), tous dirigés par leur propre DGI, gèrent également les besoins en TI considérés comme propres à un groupement de ministères. Ces groupements ne font pas partie du Bureau du DGIFP. Les employés regroupés sont des membres du personnel des ministères qui relèvent d'un sous-ministre. L'**annexe 2** consigne les personnes qui supervisaient des groupements de TI en septembre 2022.

Les huit groupements de TI fournissent des services de TI personnalisés en fonction des besoins uniques d'un ministère, qu'ils soient de portée quotidienne ou à plus long terme. Il peut s'agir de mettre en œuvre de nouveaux projets de TI, de superviser le développement, de mettre à l'essai et de mettre en œuvre des systèmes de TI, de gérer des ressources de TI et des services de consultation en TI. Par exemple, le Groupement des services à la collectivité gère le soutien en TI pour le ministère de l'Éducation, le ministère des Collèges et Universités, le ministère des Affaires municipales et du Logement, et le ministère des Industries du patrimoine, du sport, du tourisme et de la culture. Le groupement a mis au point et maintenu les systèmes informatiques nécessaires pour fournir des rapports sur la COVID-19 dans les écoles et un programme de modernisation d'Internet pour les écoles.

La **figure 2** présente la structure organisationnelle et hiérarchique du Bureau du DGIFP par rapport aux huit groupements de TI, tandis que l'**annexe 3** énumère les responsabilités du Bureau du DGIFP par rapport aux groupements.

### 2.2.1 Comités de gouvernance

Le Bureau du DGIFP, qui est régi par les conseils et comités de gouvernance des TI, examine la prestation des services de TI du Bureau du DGIFP, les politiques et la valeur des services fournis. Les comités et conseils de gouvernance suivants ont été mis sur pied pour assurer la surveillance des opérations de TI.

#### Comité exécutif de la feuille de route de la technologie de l'information

Le mandat du Comité exécutif de la feuille de route de la technologie de l'information est d'assurer le leadership et la gouvernance au niveau fonctionnel de l'organisation des TI en favorisant une meilleure compréhension des orientations en TI et des partenariats entre les fonctions d'affaires et des TI. Le comité appuie également le perfectionnement des professionnels des TI au sein de la fonction publique de l'Ontario et le fonctionnement efficace de l'organisation des TI. Il est également responsable de l'élaboration et de la mise en œuvre des normes et solutions de TI d'entreprise, le cas échéant.

#### Comité de gouvernance du programme Feuille de route technologique et plan d'investissement

Le Comité de gouvernance du programme Feuille de route technologique et plan d'investissement a pour but

## Figure 2 : Structure hiérarchique des TI dans le secteur public de l'Ontario au 19 août 2022

Préparée par le Bureau de la vérificatrice générale de l'Ontario

**Ministère des Services au public et aux entreprises (MSPE)**

**Ministre**
**Sous-ministres**

**Bureau du directeur général de l'information pour la fonction publique (Bureau du DGIFP)**
**ETP : 18**
**Paiement à l'acte : 0**

**Division de la cybersécurité (DCS)**
**ETP : 73**
**Paiement à l'acte : 11**

**Prestation en matière de technologie pour la FPO (PTF)**
**ETP : 69**
**Paiement à l'acte : 51**

**Stratégie en matière de technologie pour la FPO (STF)**
**ETP : 34**
**Paiement à l'acte : 0**

**Services technologiques d'infrastructure (STI)**
**ETP : 962**
**Paiement à l'acte : 52**

| Groupements TI | Ministères |
|---|---|
| **Groupement des organismes centraux (GOC)**<br>**ETP : 523**<br>**Paiement à l'acte : 107** | • Bureau du Conseil des ministres<br>• Cabinet du premier ministre<br>• Ministère des Finances<br>• Ministère des Affaires intergouvernementales<br>• Secrétariat du Conseil du Trésor |
| **Groupement des services de santé (GSS)**<br>**ETP : 453**<br>**Paiement à l'acte : 292** | • Ministère de la Santé<br>• Ministère des Soins de longue durée |
| **Services technologiques de la justice (STJ)**<br>**ETP : 343**<br>**Paiement à l'acte : 254** | • Ministère du Procureur général<br>• Ministère du Solliciteur général<br>• Ministère des Services à l'enfance et des Services sociaux et communautaires |
| **Groupement pour les terres et les ressources (GTR)**<br>**ETP : 194**<br>**Paiement à l'acte : 62** | • Ministère de l'Agriculture, de l'Alimentation et des Affaires rurales<br>• Ministère du Développement du Nord, des Mines, des Richesses naturelles et des Forêts<br>• Ministère de l'Environnement, de la Protection de la nature et des Parcs<br>• Ministère des Affaires autochtones<br>• Ministère de l'Énergie |
| **Groupement pour le travail et les transports (GTT)**<br>**ETP : 337**<br>**Paiement à l'acte : 318** | • Ministère du Travail, de l'Immigration, de la Formation et du Développement des compétences<br>• Ministère des Transports |
| **Groupement pour l'intégration des services gouvernementaux (GISG)**<br>**ETP : 287**<br>**Paiement à l'acte : 113** | • Ministère du Développement économique, de la Création d'emplois et du Commerce<br>• Ministère des Affaires francophones<br>• Ministère des Services gouvernementaux et des Services aux consommateurs<br>• Ministère de l'Infrastructure<br>• Ministère des Services aux aînés et de l'Accessibilité |
| **Groupement pour les services à la collectivité (GSC)**<br>**ETP : 273**<br>**Paiement à l'acte : 141** | • Ministère de l'Éducation<br>• Ministère des Industries du patrimoine, du sport, du tourisme et de la culture<br>• Ministère des Affaires municipales et du Logement<br>• Ministère de la Formation et des Collèges et Universités |
| **Groupement pour les services sociaux et les services à l'enfance et à la jeunesse (GSSSEJ)**<br>**ETP : 380**<br>**Paiement à l'acte : 372** | • Ministère des Services à l'enfance et des Services sociaux et communautaires |

d'offrir un soutien stratégique complet à l'évolution, à la surveillance et à l'orientation continues de la feuille de route technologique et du plan d'investissement du gouvernement. Le comité communique de l'information et des mises à jour à la haute direction, et précise et communique les responsabilités relatives à l'habilitation technologique et aux investissements. Il surveille, approuve et appuie les grandes initiatives.

## 2.3 Centres de données de Guelph et de Kingston

Le Centre de données de Guelph (centre de traitement de l'information) est une installation physique utilisée par la FPO pour héberger des serveurs et des bases de données d'environ 1 200 systèmes de TI. Il s'agit notamment des systèmes de TI essentiels qui servent à assurer la continuité et la prestation efficace des services gouvernementaux. En outre, certains organismes du secteur parapublic et de la Couronne ont recours au centre de traitement de l'information pour stocker leurs données, y compris la Régie des alcools de l'Ontario, Santé Ontario, l'Office des normes techniques et de la sécurité, le service de santé publique de Wellington-Dufferin-Guelph, Metrolinx et l'Autorité ontarienne de réglementation des services financiers. Le centre de traitement de l'information a été construit en 2011 parce que le centre de traitement de l'information de l'époque, situé à Toronto, avait atteint sa fin de vie utile et ne pouvait pas répondre aux exigences en matière de capacité et de disponibilité des systèmes de TI de la FPO. La FPO a également recours à une installation physique secondaire plus petite, le Centre de données de Kingston, qui héberge environ 260 systèmes de TI. Le Bureau du DGIFP est en train de transférer les systèmes de TI qui se trouvent actuellement à Kingston au Centre de données de Guelph ainsi qu'à un fournisseur de services infonuagiques. D'ici mai 2025, le Centre de données de Kingston devrait cesser ses activités.

### 2.3.1 Gestion de la reprise après sinistre

Une stratégie de reprise après sinistre (RS), qui constitue une composante de la gestion des risques de TI, sert à évaluer si un système de TI peut être restauré ou rendu fonctionnel lors de divers scénarios de catastrophe (p. ex. des pannes de courant, des cyberattaques et des tremblements de terre). Les stratégies de reprise après sinistre sont établies par chaque ministère pour déterminer les priorités et établir un calendrier de reprise. Une fois la stratégie de reprise après sinistre finalisée, un plan de reprise après sinistre est créé pour documenter étape par étape le processus de reprise des activités et services essentiels à la suite d'un scénario de catastrophe. Il est préférable qu'un plan de reprise après sinistre soit examiné, mis à l'essai et actualisé au moins une fois par année.

## 2.4 Gestion des risques dans la FPO

Le Bureau du directeur général de la gestion des risques (directeur général de la gestion des risques) de la province de l'Ontario a mis en place un processus de gestion globale des risques (GGR) par lequel les groupements de TI, le Bureau du DGIFP et les ministères cernent et déclarent les risques. Le poste de directeur général de la gestion des risques a été créé en avril 2021, et son titulaire relève du Bureau du contrôleur général au sein du Secrétariat du Conseil du Trésor. Dans le cadre du processus de GGR, le DGIFP a entamé une collaboration avec le directeur général de la gestion des risques afin de cerner divers risques liés à la cybersécurité et à la gestion des biens de TI. Chaque risque de TI documenté dans le registre des risques se voit attribuer un responsable du risque chargé de surveiller ce risque jusqu'à ce qu'il soit corrigé ou atténué.

La GGR définit les processus en place pour les principaux secteurs de contrôle d'une organisation afin de s'assurer que les risques ont été adéquatement cernés, traités ou atténués et pris en compte, y compris les risques liés aux opérations de TI et à la cybersécurité. La GGR est un mode de gestion globale qui tient compte des aspects de risque des investissements en TI, des responsabilités en matière

de gestion des risques, de la méthodologie d'analyse des risques, des stratégies de gestion des risques, de la surveillance continue des menaces, de l'occurrence et de l'incidence.

Il incombe au directeur général de la gestion des risques de l'Ontario :

- de superviser le processus de gestion globale des risques de la FPO, ce qui comprend l'examen de l'information sur les risques et des pratiques de gestion des risques du Ministère et la formulation de conseils à ce sujet;
- de fournir des conseils et de la formation et de tenir lieu de centre d'expertise à l'appui de la Directive sur la gestion globale des risques et du cadre de gestion globale des risques de la FPO;
- de fournir des conseils et une orientation lorsque les autres secteurs de programme peuvent faire face aux risques dans les directives et politiques municipales nouvelles ou existantes;
- de conseiller le secrétaire du Conseil du Trésor/Conseil de gestion du gouvernement sur l'obligation pour les ministères et les organismes provinciaux de communiquer l'information sur les risques aux organismes centraux;
- de travailler en collaboration avec les ministères et les organismes centraux pour veiller à ce que le Conseil du Trésor/Conseil de gestion du gouvernement et d'autres décideurs clés aient accès à l'information sur les risques pour éclairer la prise de décisions.

## 2.5 Gestion des biens dans la FPO

La gestion des biens comprend la surveillance et l'administration des ressources nécessaires pour fournir l'infrastructure et les services liés aux systèmes de TI. Cela comprend la gestion du cycle de vie du matériel et l'utilisation d'outils pour gérer et permettre les rapports sur les biens.

La Division des STI du Bureau du DGIFP gère trois catégories de biens :

- **Les biens informatiques d'utilisateur final** sont des appareils utilisés par le personnel de la FPO, comme les ordinateurs portables, les ordinateurs de bureau, les appareils mobiles et les tablettes. Ces biens sont suivis et stockés dans la base de données sur la gestion de la configuration (BDGC), un dépôt central qui stocke l'information relative aux biens de TI.
- **Les biens d'exploitation des centres de traitement de l'information** comprennent les serveurs, les dispositifs de stockage, le matériel et les logiciels de sauvegarde utilisés dans les deux centres de traitement de l'information. Le Bureau du DGIFP assure le suivi de ces biens dans la BDGC.
- **Les biens de télécommunications** comprennent les services de réseau et de téléphonie, comme les services d'accès à distance, les systèmes téléphoniques et les téléphones satellites.

## 2.6 Consultants en TI

Le Bureau du DGIFP a recours à la société Flextrack pour trouver des consultants en TI rémunérés à l'acte. Le contrat conclu avec Flextrack est évalué à 600 millions de dollars sur cinq ans. Flextrack a commencé à fournir des services contractuels de consultants en TI en octobre 2020, conjointement avec le fournisseur attitré de l'époque.

Au Bureau du DGIFP, lorsque des consultants en TI sont requis, une demande de services est envoyée à Flextrack à l'aide du Système de gestion des fournisseurs (SGF), un système de TI utilisé pour le traitement et l'actualisation des documents relatifs aux fournisseurs. Le SGF appartient à Flextrack et utilise un logiciel basé sur Salesforce. Le gestionnaire demandeur présente une demande sur la plateforme. Flextrack reçoit automatiquement la demande par l'entremise du VMS, après avoir d'abord vérifié le bassin existant de consultants en TI dans le système de TI. Flextrack dispose d'une liste de 359 entreprises, appelées entreprises qualifiées en TI, qui sont autorisées à soumettre des candidats pour la demande de contrat. Flextrack procède ensuite à un examen initial des curriculum vitae pour en arriver à une courte liste de candidats en fonction de leur compatibilité avec le

poste. Cette liste est ensuite envoyée au gestionnaire demandeur et aux évaluateurs d'entrevue pour évaluation.

L'évaluation subséquente consiste en un examen du curriculum vitae du candidat. Le candidat doit obtenir une note minimale de 70 % sur son curriculum vitae pour pouvoir passer à l'entrevue. Celle-ci est ensuite effectuée par au moins trois évaluateurs équivalents temps plein qui attribuent chacun une note. Le candidat qui obtient la note combinée la plus élevée de son entrevue et de son taux de rémunération quotidien décroche le contrat et se soumet à l'autorisation de sécurité et à la vérification des antécédents applicables. La **figure 3** illustre un diagramme du processus d'admission à la rémunération à l'acte.

### 2.6.1 Taux de rémunération et de paiement

Le gestionnaire responsable de l'embauche établit un taux journalier pour l'embauche en fonction des taux maximums journaliers par rôle établis par le Secrétariat du Conseil du Trésor. (Voir le tableau à l'**annexe 4.**) Pour terminer le processus d'approvisionnement, le Secrétariat du Conseil du Trésor, le GOC et le ministère demandeur sont avisés du prix, et l'équipe des finances soumet les factures de paiement à Flextrack.

Les paiements sont effectués conformément aux feuilles de temps du consultant. Le GOC effectue un rapprochement des heures soumises par l'employé contractuel et du paiement versé à Flextrack mensuellement. La FPO verse ensuite un paiement à Flextrack, qui paie par la suite la firme qualifiée en TI. Celle-ci rémunère ensuite le consultant.

### 2.6.2 Feuilles de temps et évaluation du rendement

Planview, un système du Secrétariat du Conseil du Trésor, est le système de TI actuellement utilisé pour

**Figure 3 : Processus d'embauche de consultants en TI**

Préparée par le Bureau de la vérificatrice générale de l'Ontario

1. Le gestionnaire responsable de l'embauche envoie une demande de personnel contractuel de TI à Flextrack au moyen du système de gestion des fournisseurs (SGF)
2. Le SGF vérifie la disponibilité des ressources déployables. S'il n'y en a pas, la demande est transmise à Flextrack
3. Flextrack reçoit la demande et la publie pour que toutes les entreprises qualifiées en technologie de l'information (EQTI) puissent présenter une soumission dans le SGF
4. Flextrack recueille les demandes de soumissions auprès des EQTI
5. Flextrack passe en revue les candidatures et sélectionne les candidats
6. Flextrack envoie une courte liste de candidats au gestionnaire recruteur
7. Le gestionnaire recruteur et d'autres évaluateurs évaluent le curriculum vitæ des candidats
8. Tout candidat dont le CV a obtenu une note de 70 % ou plus passe à l'étape de l'entrevue
9. Les candidats sont interviewés par trois évaluateurs équivalents temps plein
10. Le poste est attribué au candidat ayant obtenu la note globale la plus élevée (combinaison de sa note d'entrevue et de son taux de rémunération quotidien)

saisir, gérer et tenir à jour les feuilles de temps des employés contractuels et des TI de la FPO au sein des ministères. À la fin de la période de travail d'un employé, le supérieur hiérarchique effectue un sondage pour évaluer son rendement. Flextrack communique les résultats du sondage au GOC.

### 2.6.3 Système de TI pour l'approvisionnement et l'évaluation

Le statut d'évaluation du candidat est affiché dans le SGF et, lorsqu'un candidat est sélectionné, l'offre est soumise au moyen du SGF. Les approbations des énoncés de travail et des contrats attribués sont également saisies et stockées dans le SGF. Ces documents sont signés au moyen de la fonction de signature électronique DocuSign dans le cadre d'un flux de travail automatique.

## 2.7 Surveillance de la prestation des services

Les systèmes de TI sont essentiels au fonctionnement continu des services et programmes offerts par le gouvernement. Toute perturbation des opérations ou panne des principaux systèmes de TI peut avoir une incidence importante sur la disponibilité et l'exécution efficace des opérations de la FPO sur la population ontarienne. Il importe donc que les services soient fournis et que tous les incidents de TI soient résolus conformément aux ententes sur les niveaux de service prévues, ce qui devrait être conforme aux pratiques exemplaires de l'industrie.

La prestation des services est établie et exécutée dans le cadre de plusieurs ententes entre le Bureau du DGIFP, les groupements et les ministères. Ces ententes établissent les attributions rattachées au travail qui devrait être exécuté par le Bureau du DGIFP.

Celui-ci a établi une cible de conformité de 90 % pour tous les billets de prestation de services liés à des incidents de TI comme la réinitialisation des mots de passe, la restauration après des pannes du système, l'installation du logiciel de TI et l'administration des comptes utilisateurs.

# 3.0 Objectif et étendue de l'audit

Notre audit visait à déterminer si le Bureau du directeur général de l'information pour la fonction publique (DGIFP) dispose des processus et des procédures efficaces pour assurer ce qui suit :

- Un cadre de gouvernance est en place et englobe une stratégie globale de TI qui démontre une surveillance efficace des fonctions de TI afin de fournir des services de TI à la fonction publique de l'Ontario et aux Ontariens de façon efficiente et efficace.
- Les opérations et systèmes de TI sont surveillés de manière efficace conformément aux mesures de rendement établies, et des mesures correctives sont prises après examen.
- Les données et les biens de TI des Ontariens, y compris le matériel et les logiciels, sont sécurisés, fiables et protégés contre les cyberattaques.
- Les ressources de TI, y compris les employés contractuels dans ce domaine, sont acquises conformément aux exigences législatives, réglementaires et contractuelles et en tenant dûment compte de l'économie.

Dans la planification de notre travail, nous avons établi les critères que nous utiliserions pour atteindre notre objectif (voir l'**annexe 5**). Ces critères sont fondés sur un examen des lois, des politiques et des procédures applicables, ainsi que sur des études internes et externes et des pratiques exemplaires. La haute direction du Bureau du DGIFP a examiné notre objectif d'audit et les critères connexes et a convenu de leur pertinence.

Notre audit s'est déroulé de janvier à septembre 2022. Nous avons obtenu une déclaration écrite de la direction indiquant que le 23 novembre 2022, elle nous avait transmis toute l'information qui avait été portée à sa connaissance et qui pouvait sensiblement influer sur les constatations ou la conclusion du présent rapport.

Nous avons interviewé des cadres supérieurs du Bureau du directeur général de l'information pour la fonction publique relevant du ministère des

Services au public et aux entreprises pour examiner leurs attributions en matière de surveillance et d'administration des activités quotidiennes de TI à la FPO et d'exécution efficace des programmes gouvernementaux. Nous avons interviewé le directeur général de la sécurité de l'information pour déterminer si des politiques et des processus sont en place pour protéger la sécurité et la confidentialité des données confidentielles. Nous avons interviewé les cadres supérieurs de la Division de la cybersécurité du Bureau du DGIFP afin de déterminer si des analyses et des évaluations adéquates en matière de cybersécurité sont effectuées pour cerner et atténuer les risques de TI dans le portefeuille des systèmes de TI du gouvernement de l'Ontario. Nous avons interviewé des intervenants chargés de la gestion des biens de TI au sein de la FPO pour établir si l'inventaire de ces biens est tenu à jour à l'appui de la détermination des risques et des décisions d'investissement dans les biens essentiels.

Nous avons également interviewé le personnel de la haute direction des groupements et du Secrétariat du Conseil du Trésor afin de comprendre le processus d'acquisition d'employés occasionnels et de déterminer si le Bureau du DGIFP a embauché des employés contractuels en TI dans le respect des principes d'économie. Nous avons sélectionné un échantillon de 30 employés contractuels en TI et examiné les pratiques d'embauche, notamment la présélection des candidats, les notes d'entrevue, les critères de sélection des candidats et les évaluations du rendement.

Nous avons mené un sondage auprès de 51 dirigeants des TI travaillant au sein des 8 groupements de TI pour comprendre le modèle opérationnel existant et les possibilités d'amélioration des opérations et des services de TI exécutés par le Bureau du DGIFP. Nous voulions également comprendre les points de vue des intervenants sur la stratégie globale du Bureau du DGIFP, les pratiques de cybersécurité, la surveillance des fournisseurs de TI et l'acquisition des systèmes de TI. Nous avons invité les DGI des groupements, les directeurs et les responsables du processus de gestion à participer et avons obtenu un taux de réponse de 76 % (39 sur 51).

Nous avons visité le Centre de données de Guelph, qui stocke les données financières et confidentielles des Ontariens, pour évaluer la sécurité physique, les contrôles environnementaux, la sécurité et les procédures d'urgence ainsi que les procédures d'intervention en cas d'incident de TI. Nous n'avons pas visité le Centre de données de Kingston puisqu'il est en voie d'être mis hors service.

Au cours des deux prochaines années, nous prévoyons auditer les huit groupements de TI pour déterminer si les systèmes et les activités de TI sont gérés de manière efficace et efficiente et en tenant dûment compte de l'économie. La **figure 4** illustre l'étendue prévue de l'audit des TI dans la FPO par notre Bureau.

# 4.0 Constatations détaillées de l'audit

## 4.1 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

Conformément au mandat du Bureau du DGIFP, il lui incombe de s'assurer que les systèmes de TI du gouvernement provincial fonctionnent de manière efficiente et efficace en appuyant les initiatives et projets de TI de tous les ministères. Dans le cadre de ce mandat général, le Bureau du DGIFP est directement responsable des besoins en TI à l'échelle de la FPO, comme l'acquisition de biens de TI, la cybersécurité et la conception de politiques et de normes de TI. Plus précisément, son mandat consiste à optimiser les ressources de l'infrastructure technologique qui alimente l'ensemble du gouvernement et à assurer la confidentialité, la sécurité et l'intégrité de l'information, des opérations, des réseaux et des systèmes essentiels du gouvernement. Le Bureau du DGIFP supervise également les activités quotidiennes des deux centres de traitement de l'information de la FPO.

## Figure 4 : Étendue de l'audit sur la technologie Internet dans l'ensemble du service publique de l'Ontario

Préparée par le Bureau de la vérificatrice générale de l'Ontario


Le Bureau du DGIFP élabore des politiques et des normes de TI pour la FPO, notamment en ce qui concerne la sécurité de l'information, le développement d'applications et les normes de gestion des bases de données, et les fournit aux huit groupements de TI. Les priorités et objectifs, la dotation et le financement ministériels relèvent toutefois des sous-ministres associés à chaque groupement. Par conséquent, le Bureau du DGIFP n'est pas en mesure de jauger le rendement des systèmes de TI propres aux groupements. En outre, les décisions clés concernant les TI qui sont prises dans les groupements – comme la protection des données des Ontariens ou l'approvisionnement en TI de moins de deux millions de dollars conformément à sa politique, qui énonce les exigences de gestion du cycle de vie des projets de TI, telles que définies par le Secrétariat du Conseil du Trésor – ne sont pas supervisées par le Bureau du DGIFP, qui ne peut donc pas en tenir les groupements responsables. Les projets de TI dont la valeur est d'au moins deux millions de dollars doivent obtenir l'approbation du Conseil du Trésor/Conseil de gestion du gouvernement et peuvent faire l'objet de rapports trimestriels sur leur situation et leurs risques.

La structure hiérarchique actuelle, dans laquelle les groupements relèvent de leurs sous-ministres respectifs et le Bureau du DGIFP relève du ministère des Services au public et aux entreprises, ne permet pas d'exercer la surveillance nécessaire pour atténuer les risques globaux associés aux activités quotidiennes de TI dans la FPO. En conséquence, le Bureau du DGIFP est incapable de remplir son mandat. Notre sondage auprès du personnel du groupement a révélé que 92 % des répondants estimaient que la stratégie globale du Bureau du DGIFP fournit une vision appropriée pour l'avenir. Toutefois, 43 % des répondants étaient insatisfaits de leur relation avec le Bureau du DGIFP et ont indiqué que même si la stratégie est en cours, ils aimeraient être davantage mobilisés et intégrés à cette vision.

Lorsque nous avons demandé si certains services non offerts par le Bureau du DGIFP à l'heure actuelle seraient utiles dans les activités quotidiennes, 18 des 39 répondants (soit 46 %) ont indiqué que la collaboration entre les groupements et l'approvisionnement centralisé en TI favoriserait une gestion plus efficace des projets et de la capacité de TI. Seulement 13 des 39 répondants (33 %) ont déclaré avoir toujours fait participer le Bureau du DGIFP aux décisions d'approvisionnement au cours des cinq dernières années.

Compte tenu de la structure hiérarchique actuelle des groupements de TI – qui relèvent de leurs sous-ministres respectifs plutôt que du Bureau du DGIFP – nous avons relevé un certain nombre de contraintes qui l'empêchaient de s'assurer que les groupements mettent en œuvre leurs systèmes de TI de manière efficace et efficiente. Voici quelques exemples clés :

### Les normes de cybersécurité visant à sécuriser les données sensibles ne sont pas appliquées

Le Bureau du DGIFP a établi une norme de sécurité qui exige que les ministères et les groupements de TI chiffrent les données sensibles du gouvernement et de la population ontarienne. Nous avons toutefois constaté que le Bureau du DGIFP ne peut s'assurer que les groupements sécurisent les données comme l'exige la norme. Au cours de notre audit, nous avons repéré des systèmes de TI censés chiffrer des renseignements confidentiels qui n'étaient pas chiffrés. Consultez la **section 4.6.1** pour connaître les détails de cette constatation.

### Il n'existe aucune stratégie relative à l'effectif pour partager efficacement les ressources internes de TI

Étant donné que les groupements relèvent de leurs sous-ministres respectifs, leur personnel de TI respectif est cloisonné au sein de leur groupement désigné. En raison de l'approche cloisonnée, aucune stratégie relative à l'effectif de TI à l'échelle de la FPO n'a été élaborée. Compte tenu du mandat du Bureau du DGIFP, une telle stratégie permettrait au personnel de TI ayant des compétences similaires d'être réparti entre le Bureau du DGIFP et les huit groupements de TI. Les résultats de notre sondage sur les TI ont révélé que 90 % des répondants estimaient qu'ils ne disposaient pas de ressources suffisantes en TI. Les répondants ont souligné que la collaboration entre les groupements et le partage du personnel des TI comptent parmi les services que le Bureau du DGIFP pourrait offrir.

La collaboration entre les groupements et le Bureau du DGIFP pourrait permettre de réaliser des gains d'efficience et d'exercer la capacité de répondre à la demande accrue de ressources de TI. Par exemple, le Bureau du DGIFP a dirigé une équipe intergouvernementale réunissant divers groupements pour désigner 30 employés de TI de la FPO qui offriront une aide temporaire au groupement des services de santé, à l'appui du programme de vaccination contre la COVID-19 et des fonctions de soutien des systèmes, de formation et de communication.

### Il n'y a aucune surveillance des fournisseurs de TI engagés par les groupements pour des marchés de moins de deux millions de dollars

Les projets des groupements dont le coût estimatif est de deux millions de dollars ou plus sont examinés par le Bureau du DGIFP conformément à la politique définie par le Secrétariat du Conseil du Trésor, qui énonce les exigences de gestion du cycle de vie des projets de TI. Toutefois, en deçà de ce seuil, le personnel du groupement n'est pas tenu d'obtenir les commentaires ni l'approbation du Bureau du DGIFP. Par conséquent, le Bureau du DGIFP ignore souvent quels fournisseurs de TI ont été retenus, si leurs antécédents de rendement ont été pris en compte pendant la sélection et si l'approvisionnement a été conforme à la directive sur l'approvisionnement de la FPO. Sans connaître ces décisions liées aux TI, le Bureau du DGIFP ne peut pas tenir les groupements responsables des décisions en question.

Notre audit a révélé que du 1er avril 2017 au 31 mars 2022, quelque 34 fournisseurs de TI ont offert des services de TI en double ou des services semblables au Bureau du DGIFP et aux 8 groupements. Nous avons constaté qu'il n'y avait aucune vérification du rendement antérieur avant l'approvisionnement, ni aucune mise à profit des contrats existants.

Notre audit a également confirmé que le Bureau du DGIFP n'évalue pas le rendement des fournisseurs pour les approvisionnements auxquels il participe. En revanche, la majorité (64 %) de nos répondants au sondage travaillant dans les groupements nous ont dit qu'ils évaluaient effectivement le rendement des fournisseurs. Ces répondants ont également indiqué (dans une proportion de 74 %) qu'ils ne partageaient pas leurs évaluations avec le Bureau du DGIFP ni avec tout autre groupement. Il n'existe pas de répertoire central où sont consignés les résultats d'un fournisseur,

qui pourrait être consulté et utilisé par les groupements ou le Bureau du DGIFP pour déterminer si ce fournisseur devrait être réembauché.

## RECOMMANDATION 1

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 (le 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 devrait :

- 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.

## RÉPONSE DU MINISTÈRE

Le Ministère et le Secrétariat du Conseil du Trésor acceptent la recommandation de la vérificatrice générale et s'engagent à mettre en place une gouvernance adéquate pour assurer l'optimisation des ressources. À cet égard, le Secrétariat du Conseil du Trésor et le Ministère s'engagent à :

- collaborer avec les groupements pour examiner les structures de gouvernance et les rapports hiérarchiques des DPI des groupements dans le contexte d'autres considérations opérationnelles, structurelles et de leadership, et prendre les mesures nécessaires pour assurer la mise en place d'une gouvernance et d'une responsabilisation adéquates;
- 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 et les inclure dans le nouveau modèle intégré de gouvernance numérique et de TI en cours d'établissement afin de régir la technologie de l'information et les solutions numériques à haut risque au sein de la fonction publique de l'Ontario.

## 4.2 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

Dans le cadre du processus de détermination des risques, les ministères, les groupements de TI et le Bureau du DGIFP sont chargés de relever les risques liés aux TI pour leur propre portefeuille et de les signaler trimestriellement au Bureau du directeur général de la gestion des risques (le directeur général de la gestion des risques). En août 2022, le directeur général de la gestion des risques tenait un registre des risques qui comprenait 38 risques liés aux TI, comme la cybersécurité, la confidentialité des données et les systèmes de TI vieillissants, qui ont été recensés par les ministères et les groupements. Chaque risque est classé comme élevé, moyen-élevé, moyen ou faible.

Nous avons rencontré le directeur général de la gestion des risques de l'Ontario pour examiner les risques liés aux TI qu'il surveille pour la FPO. Nous avons appris que le Bureau du DGIFP n'avait pas cerné ni évalué de risques liés aux TI dans son propre secteur d'activité. De plus, le DGIFP s'est fié aux ministères et aux groupements pour cerner les risques en matière de TI. Après examen, nous avons constaté que le seul risque de TI du registre jugé élevé était un risque de cybersécurité identifié dans l'audit de 2018 de notre Bureau intitulé Conseils scolaires – Systèmes de TI et technologie en salle de classe.

De plus, nous avons remarqué que les groupements et les ministères ne communiquent pas au Bureau du DGIFP leurs risques respectifs en matière de TI ni ne les informent à cet égard. Même si le Bureau du DGIFP assume la responsabilité globale des TI au sein de la FPO (conformément à son mandat), il n'identifie,

ne documente ni ne communique pas les risques systémiques de TI et les facteurs d'atténuation à la FPO, pas plus qu'il n'effectue une évaluation indépendante de ces risques de TI ni n'évalue l'incidence globale sur l'ensemble de la FPO.

Nous avons également comparé les risques de TI énumérés dans le registre des risques de la FPO aux risques de TI standard de l'industrie et constaté qu'aucun des principaux risques prévus n'avait été relevé. Par exemple, l'Open Web Application Security Project (OWASP), une fondation sans but lucratif de premier plan, publie les principaux risques de cybersécurité qui touchent les industries à l'échelle mondiale. Aucun des 10 principaux risques de cybersécurité de l'OWASP, comme la mauvaise configuration de la sécurité, le manque de chiffrement et la conception non sécurisée, n'était présent dans le registre des risques de TI de la FPO. Nous avons constaté que d'autres risques clés en matière de TI associés au vieillissement des systèmes de TI, à la sécurité des données, à l'absence de plans de reprise après sinistre et aux risques associés aux fournisseurs tiers étaient également absents. Consultez les **sections 4.4**, **4.6** et **4.7** pour connaître nos conclusions sur la reprise après sinistre, la cybersécurité et la gestion des biens de TI, respectivement.

Au Bureau du DGIFP, le processus actuel de gestion des risques n'est pas parvenu à maturité et n'a pas de stratégie officielle pour identifier et gérer les risques de TI. Au moment de notre audit, le Bureau du DGIFP était en train d'établir un nouveau cadre et une nouvelle stratégie pour collaborer avec le directeur général de la gestion des risques afin de cerner, de documenter et de communiquer les risques de TI à la FPO dans le cadre du processus de gestion globale des risques.

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

### RÉPONSE DU MINISTÈRE

Le Ministère souscrit à cette recommandation et reconnaît l'importance de cerner, de signaler et d'atténuer les risques liés aux TI à l'échelle organisationnelle.

À cet égard, le Ministère s'engage à :

- peaufiner son processus de production de rapports sur les risques et à collaborer avec le Bureau du directeur général de la gestion des risques pour établir un nouveau cadre aligné sur la stratégie de TI qui englobe les risques organisationnels en matière de TI et les risques déclarés par les groupements de TI au Bureau du DGIFP;
- veiller à ce que le Bureau du DGIFP assure le suivi de tous les risques liés aux TI et à ce que des mesures soient en place pour les atténuer. Les groupements de TI continueront de jouer un rôle dans la détermination et l'atténuation des risques propres à leurs projets de TI en soutien aux ministères;
- examiner les normes existantes de l'industrie afin de s'assurer que les risques en matière de TI organisationnelles figurant dans le registre des risques sont pertinentes et à jour.

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

Le Centre de données de Guelph du gouvernement a coûté un total de 352 millions de dollars et

est opérationnel depuis le 31 mars 2011. Son fonctionnement coûte en moyenne 9 millions de dollars par année, et il appartient au ministère des Services au public et aux entreprises. La Division des STI du Bureau du DGIFP est responsable des opérations quotidiennes et de la supervision du centre de traitement de l'information, comme l'accès aux salles de serveurs et la surveillance de la capacité (stockage) et de la disponibilité (pannes) des serveurs. La superficie de l'installation est d'environ 250 000 pieds carrés et l'aire de stockage des serveurs est de 30 000 pieds carrés.

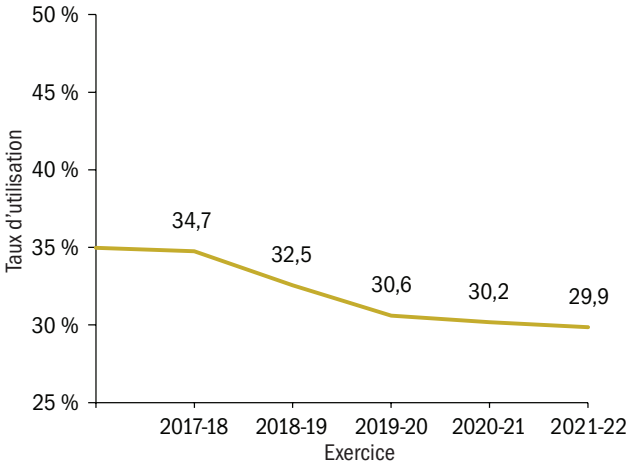
Un organisme international indépendant, l'Uptime Institute, a attribué au centre de traitement de l'information une cote de niveau IV – la note la plus élevée pour un centre de traitement de l'information. Cette cote indique que les systèmes de TI hébergés au centre de traitement de l'information certifié peuvent résister à tous les types de défaillance : matériel, CVCA ou crises environnementales comme des tremblements de terre ou des incendies. Le Centre de données de Guelph est le seul centre de traitement de l'information au Canada et le seul parmi les quatre en Amérique du Nord à obtenir cette cote.

Notre audit a révélé que le centre de traitement de l'information est considérablement sous-utilisé. Nous avons examiné les rapports d'utilisation des cinq dernières années et constaté qu'en moyenne, seulement 32 % de sa capacité d'hébergement de serveurs et de bases de données était exploitée. L'utilisation a diminué au cours de cette période, comme le montre la **figure 5a**. En août 2022, le centre de traitement de l'information utilisait seulement 30 % de l'espace disponible. Nous avons calculé qu'en raison de la sous-utilisation, le Bureau du DGIFP a engagé 31 millions de dollars supplémentaires et qu'une perte directe en coûts d'exploitation a été subie sur cinq ans pour l'électricité, le refroidissement, l'entretien et la sécurité physique de l'espace inoccupé. Ces coûts d'exploitation auraient pu être compensés par l'occupation de l'espace non utilisé par d'autres clients gouvernementaux qui auraient partagé les coûts. La **figure 5b** représente les dépenses d'exploitation des locaux utilisés et non utilisés au centre de traitement de l'information.

Bien que le centre de traitement de l'information ait été construit en mars 2011 dans le but de desservir uniquement la FPO et qu'il ait cette capacité, l'utilisation du secteur parapublic et des organismes de la Couronne est minimale à l'heure actuelle. Nous avons constaté que le Bureau du DGIFP a soumis une analyse de rentabilisation au Secrétariat du Conseil du Trésor en 2012 dans le but de tirer parti

**Figure 5a : Taux d'utilisation (%) du Centre de données de Guelph, de 2017-2018 à 2021-2022***

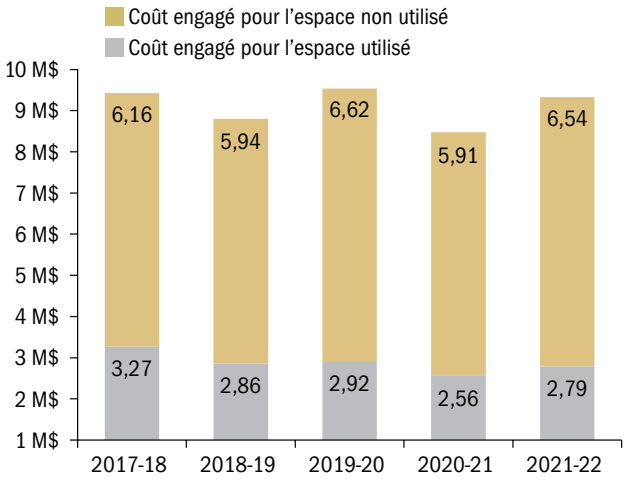
Préparée par le Bureau de la vérificatrice générale de l'Ontario




* Le taux d'utilisation est basé sur la moyenne de l'énergie (kW), du refroidissement (tonnes) et de l'espace sur les serveurs.

**Figure 5b : Charges d'exploitation du Centre de données de Guelph (en millions de dollars), de 2017-2018 à 2021-2022**

Préparée par le Bureau de la vérificatrice générale de l'Ontario



du nouveau centre de traitement de l'information à des fins d'utilisation par des organismes du secteur public à l'extérieur de la FPO en établissant un service de partage de locaux qui sera utilisé par le secteur parapublic. Cependant, le Bureau du DGIFP n'a pas établi de stratégie de marketing ni participé à des activités de sensibilisation pour mettre en valeur les capacités du centre de traitement de l'information. À l'heure actuelle, les contribuables engagent des coûts pour exploiter le centre de traitement de l'information ainsi que des coûts supplémentaires que les organismes de la Couronne paient aux entreprises privées pour des services que le centre de traitement de l'information pourrait fournir. En comparaison, le gouvernement de la Colombie-Britannique oblige son secteur parapublic, y compris les organismes de santé, à utiliser son centre provincial de traitement de l'information.

Nous avons comparé les prix des centres de traitement de l'information avec ceux du secteur privé et nous avons découvert que les frais sont généralement beaucoup plus élevés que ceux du secteur privé. Le centre de traitement de l'information facture environ 75 $ le pied carré (soit 1,33 $/kWh après conversion en électricité à des fins de comparaison) pour le coût de l'installation et des ressources, ce qui comprend la superficie, le chauffage, la climatisation, l'électricité, la sécurité physique et d'autres besoins pour exploiter l'installation en fonction de l'espace alloué. La structure des coûts des centres de traitement de l'information du secteur privé est calculée en fonction de la consommation d'électricité fondée sur l'utilisation de kilowattheures (kWh) et non sur l'utilisation de pieds carrés. Le Bureau du DGIFP a retenu les services d'un cabinet externe de consultants, Ernst & Young, pour évaluer les activités du centre de traitement de l'information. Le consultant a établi que le centre de traitement de l'information facture environ 1,33 $/kWh, soit plus du double du montant facturé par les autres exploitants privés de centres de traitement de l'information de niveau IV. Les frais moyens sont d'environ 0,59 $/kWh dans d'autres pays, comme les États-Unis, le Royaume-Uni et l'Australie. Cette analyse a également permis de déterminer que si le centre de traitement de l'information fonctionnait à 100 % de sa capacité, le coût diminuerait à 0,67 $/kWh comparativement aux frais actuels de 1,33 $/kWh.

En 2019, Élections Ontario a transféré son hébergement de données du Centre de données de Guelph à un centre de traitement de l'information infonuagique appartenant à Microsoft. Nous avons examiné les procès-verbaux des réunions de la direction et constaté que la décision avait été prise en fonction de coûts moindres, de la souplesse nécessaire pour accroître la capacité de l'infrastructure de TI pendant les cycles électoraux et du temps d'approvisionnement plus rapide pour configurer les serveurs offerts par les fournisseurs d'informatique en nuage. À l'heure actuelle, le centre de traitement de l'information n'a pas les capacités susmentionnées.

Nous avons également remarqué que le Centre de données de Kingston sera mis hors service d'ici mai 2025 et que les systèmes de TI qui y sont hébergés sont en voie d'être transférés au Centre de données de Guelph ainsi qu'à un fournisseur tiers de services d'informatique en nuage. Les systèmes de TI ne sont pas tous transférés au Centre de données de Guelph parce que le Bureau du DGIFP veut s'assurer que les systèmes de TI sont en mesure d'accroître rapidement la capacité et les fonctionnalités de reprise après sinistre. Parmi les autres défis, mentionnons le manque de normalisation des systèmes de TI dans la FPO et les compétences techniques. Le Bureau du DGIFP a reconnu ces lacunes du centre de traitement de l'information et dresse actuellement un plan pour les corriger et augmenter l'utilisation du centre de traitement de l'information. Consulter les détails à la **section 4.3.1.**

### 4.3.1 Avenir du Centre de données de Guelph

Reconnaissant la sous-utilisation du centre de traitement de l'information, le Bureau du DGIFP a retenu les services d'une firme d'experts-conseils externe, Ernst & Young (E & Y), en avril 2021, pour examiner le modèle opérationnel actuel du centre de traitement de l'information. L'examen visait à comprendre l'établissement des coûts d'exploitation des centres de traitement de l'information, à cerner

les lacunes, à comparer des centres de traitement de l'information semblables disponibles sur le marché et à formuler des recommandations en vue d'un futur modèle opérationnel qui permettrait d'accroître l'utilisation et de générer plus de revenus. Trois modèles d'exploitation différents ont été proposés dans le but d'augmenter son utilisation tout en réduisant les coûts d'exploitation. Voici quelles étaient les trois options :

- **Option 1 :** Maintenir le statu quo et continuer d'exploiter le centre de traitement de l'information tel qu'il fonctionne aujourd'hui. Élaborer une stratégie pour accroître l'utilisation du centre de traitement de l'information dans ce modèle opérationnel.
- **Option 2 :** Collaborer avec Infrastructure Ontario et le secteur privé pour exploiter et gérer le centre de traitement de l'information. Étudier les ententes de location ou de partage de bail dans le cadre desquelles la FPO sous-louerait 100 % de l'espace moyennant des frais fixes, puis en paierait l'utilisation.
- **Option 3 :** Résilier le bail et vendre le centre de traitement de l'information à un fournisseur. La FPO deviendrait l'un des locataires du centre de traitement de l'information appartenant au fournisseur.

Au moment de notre audit, le Bureau du DGIFP procédait à sa propre analyse des trois options proposées par E & Y. L'analyse visant à déterminer les options qu'il entend mettre de l'avant devrait être faite d'ici décembre 2022. On nous a informés qu'une fois son analyse terminée, le Bureau du DGIFP préparera une analyse de rentabilisation qui tiendra compte des commentaires de divers intervenants comme Infrastructure Ontario, ApprovisiOntario, Relations de travail, et des consultations numériques et privées pour évaluer le futur modèle opérationnel, puis soumettra l'analyse de rentabilisation au Secrétariat du Conseil du Trésor pour examen et approbation du financement (selon l'option retenue) dans le cadre de son processus de planification pluriannuelle 2023-2024.

### 4.3.2 Le Bureau du DGIFP ne dispose pas d'un processus pour révoquer l'accès des employés extérieurs à la FPO ayant quitté leur emploi au Centre de données de Guelph

Lors de notre examen du centre de traitement de l'information, nous avons remarqué que le Bureau du DGIFP n'avait pas établi de processus d'examen de l'accès des utilisateurs pour s'assurer que l'accès des employés au centre de traitement de l'information est révoqué en temps opportun au moment de leur départ. Le centre de traitement de l'information et le Bureau du DGIFP obtiennent périodiquement des attestations des membres de la FPO, mais non des organismes de la Couronne ou du secteur parapublic. Dans ces cas, le Bureau du DGIFP dépend uniquement des organismes de la Couronne et du secteur parapublic pour les informer de tout licenciement d'employés.

Il en résulte qu'un employé de la Régie des alcools de l'Ontario qui a été licencié en février 2022 a continué d'avoir accès au centre de traitement de l'information jusqu'à la date d'expiration de sa carte d'accès physique en juillet 2022. Le centre de traitement de l'information n'a pas établi de processus de suppression des utilisateurs pour s'assurer que les utilisateurs licenciés sont activement retirés dans les 24 heures suivant la cessation d'emploi, ce qui constitue une lacune importante du processus pour un centre de traitement de l'information de niveau IV.

## RECOMMANDATION 3

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;
- 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;
- 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;
- 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;
- 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.

### RÉPONSE DU MINISTÈRE

Le Ministère souscrit à cette recommandation visant à accroître l'utilisation du Centre de données de Guelph et à renforcer ses contrôles existants d'accès des utilisateurs et s'engage à :
- effectuer une analyse coûts-avantages qui tient compte du taux de recouvrement des coûts pour attirer et intégrer d'autres entités au centre de données;
- évaluer la faisabilité de mandater le secteur parapublic et les organismes de la Couronne pour accroître l'adoption du centre de données;
- élaborer une stratégie de sensibilisation pour le secteur parapublic et les organismes provinciaux afin d'accroître l'adoption du centre de données;
- déterminer un modèle opérationnel futur pour le Centre de données de Guelph en tenant dûment compte de l'économie et de la sécurité des données;
- élaborer un processus d'attestation pour les organismes et les fournisseurs afin que l'accès des utilisateurs soit supprimé dans les 24 heures suivant la cessation d'emploi.

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

Une stratégie de reprise après sinistre est le plan d'une organisation visant à désigner et à restaurer les systèmes de TI essentiels à son fonctionnement en cas de catastrophe ou d'interruption des services. Compte tenu des systèmes de TI utilisés dans la FPO, une catastrophe pourrait avoir une incidence sur la sécurité publique (dans le cas des systèmes de TI d'urgence 911, par exemple) ou sur les services essentiels comme les opérations de soins de santé. Une stratégie de reprise après sinistre peut faciliter la restauration des systèmes de TI le plus rapidement possible en cas de catastrophe.

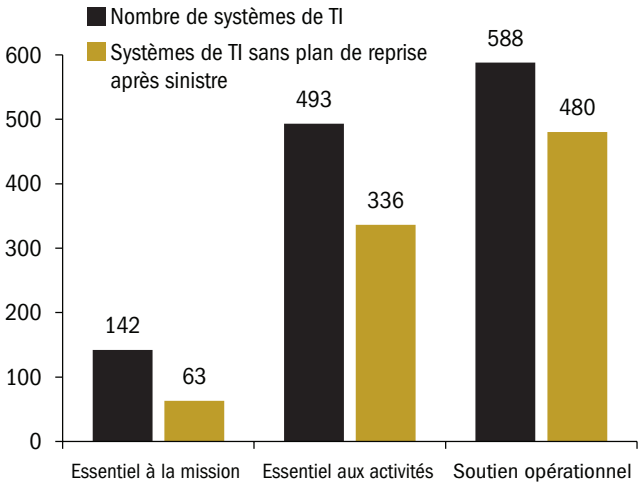
Notre audit a révélé que le Bureau du DGIFP n'avait pas conçu de stratégie ni de politique de reprise après sinistre à l'échelle de l'organisation pour les systèmes de TI de la FPO. Elle n'a pas non plus mis à l'épreuve sa capacité de rétablir les opérations de TI en cas de panne majeure semblable à la panne de Rogers survenue en juillet 2022 dont il est question à la **section 4.5**. Chaque groupement de TI est plutôt responsable de concevoir et de mettre à l'essai sa propre stratégie de reprise après sinistre, sans mettre à l'essai les dépendances possibles de ses systèmes de TI à l'égard d'autres systèmes de TI ou des services de réseau gérés par le Bureau du DGIFP.

Nous avons constaté ce qui suit :
- 63 des 142 systèmes essentiels à la mission (soit 44 %) n'ont pas de plan de reprise après sinistre;
- 336 des 493 systèmes essentiels aux opérations (soit 68 %) n'ont pas de plan de reprise après sinistre;
- 480 des 588 systèmes de soutien des activités (soit 82 %) n'ont pas de plan de reprise après sinistre.

La **figure 6** présente une ventilation des systèmes de TI sans plan de reprise après sinistre en date d'août 2022. Nous avons constaté que certains de ces systèmes de TI ont connu d'importants incidents au cours des cinq dernières années. Ces incidents ont donné lieu à des pannes imprévues qui auraient pu

### Figure 6 : Systèmes de TI sans plan de reprise après sinistre, août 2022

Préparée par le Bureau de la vérificatrice générale de l'Ontario




être évitées si une stratégie de reprise après sinistre avait été mise en place et mise à l'essai pour assurer une perturbation minimale des systèmes de TI. Par exemple :

- **Les centres de contact de la FPO ont recours au système de TI des services de soins de santé d'urgence** pour les services 911 d'urgence qui font appel à des ambulances, des hôpitaux et des transferts de patients. Nous avons noté 13 incidents critiques liés aux TI dans le cadre desquels de nombreuses lignes téléphoniques 911 ont été touchées à la fois par des problèmes de matériel et de logiciel informatique, comme des câbles réseau défectueux, des pannes d'alimentation électrique et des problèmes de rendement de l'équipement de TI. Cela a entraîné la perte de connexion entre les systèmes 911 et plusieurs centres intégrés d'expédition d'ambulances, et par conséquent des retards dans la répartition des ambulances. En moyenne, ces incidents ont été réglés en huit heures. Le temps de résolution le plus long a été de 24 heures, tandis que le temps de résolution cible est de 4,5 heures.
- **Les sites Web du visualisateur de patients atteints de la COVID-19** et **du portail sur la vaccination des patients atteints de la COVID-19** sont utilisés par les Ontariens pour s'inscrire aux rendez-vous de vaccination contre la COVID-19 et pour consulter les résultats des tests de dépistage de la COVID-19. Ces sites Web se sont butés à 18 incidents critiques liés aux TI pendant la pandémie, au cours desquels les Ontariens n'ont pas été en mesure de prendre des rendez-vous de vaccination ni de consulter leurs résultats de test. Les pannes informatiques sont survenues parce que les correctifs de maintenance n'ont pas été appliqués à temps. Il a fallu en moyenne 17 heures pour résoudre ces incidents. Le temps de résolution le plus long a été de 48 heures. Le temps de résolution requis est fixé à 4,5 heures.
- **Le Système d'information de laboratoire** est un logiciel de soins de santé utilisé par les laboratoires de santé publique pour actualiser, traiter et conserver les renseignements sur les patients associés aux procédures de laboratoire et aux résultats des tests. Nous avons constaté que six incidents critiques se sont produits en raison de problèmes de connectivité des bases de données et de problèmes de rendement qui ont entraîné des retards dans la récupération des renseignements sur les patients. En moyenne, ces incidents ont été résolus en 36,5 heures, comparativement aux 4,5 heures qui constituent le temps de résolution requis.
- **GO Secure** est utilisé par les employés et les entrepreneurs de la FPO pour accéder en toute sécurité aux systèmes de TI de la FPO. Nous avons constaté que 10 incidents critiques liés aux TI, comme le redémarrage inattendu du serveur et les problèmes de base de données, ont empêché les employés et les entrepreneurs de la FPO d'accéder aux systèmes de TI de la FPO pendant une longue période. En moyenne, ces incidents ont été résolus en 12,5 heures alors que le temps de résolution requis est de 4,5 heures.

## RECOMMANDATION 4

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

## RÉPONSE DU MINISTÈRE

Le Ministère souscrit à cette recommandation et s'engage à s'assurer que les systèmes de TI sont résilients et disponibles, tout en réduisant au minimum les interruptions des activités, au moyen d'un plan de reprise après sinistre.

Les plans de reprise après sinistre sont fondés sur des ententes sur les niveaux de service propres à chaque ministère et, par conséquent, le Ministère s'engage à :

- intégrer les plans de reprise après sinistre propres au groupement de TI dans une stratégie globale de reprise après sinistre à l'échelle de la FPO;
- collaborer avec les partenaires ministériels pour confirmer quels sont les systèmes de TI qui nécessitent un plan de reprise après sinistre, en tenant compte des plans de continuité des activités du ministère et en veillant à ce que ceux qui nécessitent un plan de reprise après sinistre en aient mis un en place dans le cadre d'ententes sur les niveaux de service établies;
- collaborer avec les partenaires ministériels pour examiner la conformité des groupements aux plans de reprise après sinistre et les mettre à l'essai annuellement ou dans l'éventualité d'un changement important dans l'environnement de TI de la FPO afin de récupérer rapidement les systèmes de TI essentiels.

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

Rogers Communications (Rogers) est l'un des plus importants fournisseurs de services de télécommunications pour la FPO et le seul fournisseur de services de réseau pour environ 128 bureaux, et assure la connectivité téléphonique pour 44 centres de contact/d'appels et les 56 000 téléphones cellulaires utilisés par tous les employés de la FPO. Le 8 juillet 2022, Rogers a connu une panne majeure à l'échelle du réseau qui a touché des milliers de Canadiens dans diverses provinces. Les clients de Rogers, y compris la FPO, se sont retrouvés sans téléphone et sans service Internet pendant plus de 15 heures. Selon l'entreprise, une erreur de codage de ses équipements de réseau a causé la panne.

Étant donné que Rogers est le seul fournisseur de services de certains services de réseau pour les principales activités essentielles de la FPO, comme les centres d'appels et les téléphones mobiles, la panne à l'échelle nationale a eu des répercussions importantes sur les activités de la FPO, qui n'a pas été en mesure de fournir des services aux Ontariens par l'entremise de centres de contact comme Service Ontario, les cliniques de vaccination contre la COVID-19 et les sites Web des paiements d'aide sociale. Bien que la majorité des bureaux de la FPO n'aient pas été touchés par la panne, le personnel de la FPO qui utilisait l'Internet à domicile de Rogers n'a pas pu accéder à Internet pour exercer ses activités quotidiennes. Le Bureau du DGIFP a évalué la perte directe de productivité à 500 000 $ en raison de l'incapacité de ces membres du personnel à

travailler. Le Bureau du DGIFP a élaboré une position opérationnelle sur ce que l'indemnisation estimative pourrait être en fonction de l'incidence sur les activités gouvernementales.

De plus, les composantes touchées comprenaient 11 systèmes de TI essentiels, 44 centres de contact, 29 systèmes de TI ministériels, 128 emplacements physiques du ministère et 56 000 téléphones cellulaires utilisés par les employés de la FPO. Parmi les 11 systèmes de TI essentiels, 5 fournissent des services d'urgence, comme le centre d'appels 911, les services d'ambulance, les avis d'incendie et les paiements essentiels aux Ontariens.

Voici quelques exemples de systèmes de TI touchés par la panne :

- Les systèmes de localisation automatique des véhicules et de répartition assistée par ordinateur mobile servent à recueillir et à partager les emplacements des ambulances, à envoyer les ambulances vers les urgences et à transférer les incidents de type 911 aux centres de répartition des ambulances. Ces systèmes informatiques dépendaient exclusivement des services de Rogers dans quatre villes : Mississauga, Cambridge, Georgian Bay et London. En raison de la panne, les centres de répartition des ambulances n'ont pas pu partager les emplacements des ambulances, et les services paramédicaux n'ont pas pu prendre de décisions opérationnelles. Comme solution de rechange, les centres de répartition ont effectué un suivi manuel des ambulances à l'aide de radios.
- Le système automatisé d'avis d'incendie est utilisé par les centres d'appels 911 pour aviser les casernes de pompiers en cas d'urgence. En raison de la panne de Rogers, les casernes de pompiers n'ont pas été en mesure de recevoir des avis automatisés d'incendie des centres de répartition. Comme solution de rechange, les casernes de pompiers ont été contactées par téléphone.
- Le Système automatisé de gestion de l'aide sociale utilisé par la province pour verser les prestations d'aide sociale n'était pas en mesure de traiter les paiements.

Quarante-quatre centres d'appels à travers la province ont aussi été perturbés. Par exemple, Santé publique Ontario et l'InfoCentre provincial pour la vaccination n'ont pas pu fonctionner pendant cette période. Les Ontariens ont également éprouvé des difficultés à communiquer avec le service à la clientèle de Service Ontario, car les communications étaient en panne. L'**annexe 6** fournit une liste des autres services de la FPO touchés par la panne de Rogers.

En général, les organisations mettent en œuvre leurs plans de continuité des opérations et de reprise après sinistre en cas de panne de réseau afin de s'assurer que les activités essentielles sont exécutées avec le moins d'interruptions possible. Comme la FPO dépendait uniquement d'un fournisseur unique de services Internet pour ses centres de contact et ses téléphones mobiles, et qu'elle n'avait pas de fournisseur de services de secours, elle n'a donc pas pu rétablir les opérations, même pour les systèmes de TI qui avaient des plans de continuité des opérations et de reprise après sinistre.

### 4.5.1 Les amendes imposées pour l'interruption de service de Rogers ne tiennent pas compte des pertes subies par la FPO

Selon l'entente de niveau de service existante entre le Bureau du DGIFP et Rogers, il conviendrait de maintenir des objectifs de rendement comme 99,9 % de disponibilité de la connexion Internet. Cette entente comporte des clauses de pénalité qui prévoient des amendes si Rogers ne fournit pas les niveaux de service convenus.

Le Bureau du DGIFP a effectué une évaluation pour déterminer les amendes qu'il convient d'imposer à Rogers. En se fondant sur les clauses de pénalité de l'entente, le Bureau du DGIFP a calculé qu'il peut imposer une amende de 38 000 $ à Rogers. De plus, le Bureau du DGIFP recevra cinq jours de crédits de service, soit environ 200 000 $, ce que Rogers a annoncé pour tous ses clients. Le Bureau du DGIFP

a toutefois évalué qu'il a subi une perte directe de 500 000 $ en productivité en raison de cette panne puisque les employés de la FPO n'ont pas pu travailler. Le Bureau du DGIFP a élaboré une position opérationnelle sur ce que la rémunération estimative pourrait être en fonction de l'incidence sur les activités gouvernementales.

Au vu de l'impact financier subi par la FPO comme conséquence directe de la panne de Rogers, les amendes imposées par le Bureau du DGIFP ne compensent pas la perte qu'il a subie. Notre audit a révélé que le contrat entre le Bureau du DGIFP et Rogers avait été conclu en 2014 et n'avait jamais été mis à jour. Le contrat existant ne permet pas au Bureau du DGIFP d'imposer des amendes en raison d'une panne globale du réseau.

### RECOMMANDATION 5

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

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

### RÉPONSE DU MINISTÈRE

Le Ministère souscrit à cette recommandation. En réponse aux recommandations de la vérificatrice générale, le Ministère s'engage à :

- sélectionner un fournisseur de réseau secondaire de secours pour les activités essentielles déterminées par le Ministère, y compris les centres de contact, les services de mobilité et les systèmes de TI;
- tenir compte des clauses de pénalité pour les nouveaux contrats de réseau et les renouvellements de contrats existants.

## 4.6 Les pratiques de cybersécurité de la FPO doivent être améliorées

La Division de la cybersécurité du Bureau du DGIFP est chargée de fournir des services de cybersécurité aux 29 ministères du gouvernement de l'Ontario. Ces services comprennent la surveillance des cyberattaques, l'exécution d'évaluations et d'analyses de cybersécurité, la prestation d'une formation sur la cybersécurité et la prestation de conseils en matière d'approvisionnement en sécurité des TI pour des services de cybersécurité au gouvernement. Bien que la FPO ait fait des progrès dans sa position globale en matière de cybersécurité, nous avons constaté qu'elle devait davantage la renforcer pour protéger les données des Ontariens avec une incidence minimale sur leur intégrité, leur sécurité et leur disponibilité.

Nous avons examiné les contrôles liés aux évaluations de cybersécurité. En raison de la nature de la cybersécurité et afin de réduire au minimum le risque d'exposition pour la fonction publique de l'Ontario, nous avons fourni des détails pertinents de nos constatations et recommandations directement au Bureau du DGIFP. Le Bureau du DGIFP a convenu du bien-fondé de la recommandation et s'est engagé à protéger les données confiées au gouvernement par la population et les entreprises de l'Ontario.

### 4.6.1 Les données sensibles ne sont pas sécurisées à l'aide de chiffrement comme il se doit

Le Bureau du DGIFP a établi une norme de sécurité qui énonce les exigences relatives au stockage sécuritaire des renseignements personnels et sensibles des Ontariens. Conformément à la norme, les renseignements personnels recueillis doivent être conservés, transférés et éliminés de façon sécuritaire afin de les protéger contre le vol, la perte ou l'utilisation ou la divulgation non autorisée.

Si les renseignements personnels recueillis par voie numérique ne sont pas protégés par le chiffrement, par exemple, ils pourraient enfreindre la *Loi sur l'accès à l'information et la protection de la vie privée*.

Nous avons sélectionné cinq systèmes de TI utilisés par le ministère des Services au public et aux entreprises, le ministère du Solliciteur général, le ministère de la Santé et le ministère de la Sécurité communautaire et des Services correctionnels qui stockent des données personnelles et sensibles des Ontariens afin de vérifier si les données étaient stockées conformément à la norme de sécurité des données requise. Nous avons découvert qu'aucun des cinq systèmes de TI échantillonnés ne disposait de contrôles de sécurité des données comme le chiffrement.

Le Bureau du DGIFP compte sur les ministères pour faire respecter les exigences en matière de sécurité des données des groupements et ne surveille pas lui-même la conformité à ces exigences. En outre, en raison de la structure hiérarchique existante des groupements pour leurs ministères respectifs (plutôt que pour le Bureau du DGIFP), le Bureau du DGIFP n'applique pas et ne surveille pas les exigences en matière de sécurité des données des groupements.

Dans le cadre de l'audit des Comptes publics de 2021-2022 mené par le Bureau de la vérificatrice générale de l'Ontario, nous avons relevé des lacunes en matière de sécurité des données en ce qui concerne les contrôles généraux de TI, comme l'administration de l'accès des utilisateurs, la gestion du changement et les opérations de TI pour les systèmes de TI gérés par des groupements de TI.

## RECOMMANDATION 6

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.

## RÉPONSE DU MINISTÈRE

Le Ministère tient à remercier la vérificatrice générale et son équipe pour leurs recommandations visant à améliorer la profondeur des pratiques de défense du programme de cybersécurité. À cet égard, il s'engage à collaborer avec les partenaires ministériels et les groupements pour examiner et mettre en œuvre des approches visant à surveiller et à faire respecter les normes de sécurité des groupements, y compris le chiffrement des données sensibles.

### 4.6.2 Sensibilisation insuffisante du personnel de la FPO à la cybersécurité

#### 4.6.2.1 La majorité des employés de la FPO ne sont pas formés aux dernières pratiques de cybersécurité

L'erreur humaine est l'une des menaces les plus importantes pour la cybersécurité d'une organisation. Selon un article paru en avril 2022 et rédigé par Gartner Inc., une société de recherche et de consultation de premier plan dans le secteur, l'erreur humaine demeure l'un des cinq principaux risques pour la sécurité à l'échelle mondiale. Une formation de base sur la sensibilisation à la cybersécurité est donc essentielle pour que les employés puissent comprendre les données avec lesquelles ils travaillent et éviter de les exposer à des pirates potentiels. En 2020, la Division de la cybersécurité du Bureau du DGIFP, par l'entremise de son Centre d'excellence en cybersécurité, a conçu un cours d'introduction à la cybersécurité à l'intention de tous les employés de la FPO pour les tenir informés des risques d'attaques liées à la cybersécurité. Tous les employés à temps plein ont accès à un système de TI appelé LearnON, où ils peuvent suivre des cours de formation conçus pour les employés du gouvernement de l'Ontario. Depuis avril 2022, le cours obligatoire « Principes de base de la cybersécurité » du Bureau du DGIFP, offert sur LearnON, aide les

employés à comprendre la classification des données et les pratiques exemplaires, comme l'utilisation appropriée du courriel, le téléchargement de pièces jointes ou de programmes externes et la façon d'éviter l'hameçonnage. Nous avons noté ce qui suit :

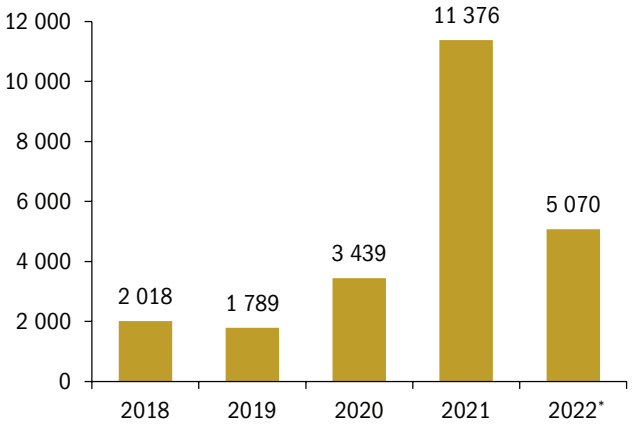
- Selon le rapport de présence au cours sur les notions de base en cybersécurité de 2018-2022, seulement 11 000 des quelque 40 000 employés de la FPO (soit moins de 30 %) ont suivi ce cours en 2021. Toutefois, depuis son lancement en 2020, le nombre d'employés de la FPO qui ont suivi la formation obligatoire en cybersécurité a augmenté. La **figure 7** présente une tendance quinquennale de la participation aux cours de cybersécurité pour tout le personnel de la FPO de 2018 à 2022.
- De 2017 à 2022, la Division de la cybersécurité a signalé un total de 33 cyberattaques, comme le montre la **figure 8**. De ces 33 attaques de cybersécurité, 27 étaient liées à un événement d'hameçonnage, c'est-à-dire qu'un employé de la FPO a cliqué sur un lien Web malveillant et fourni son nom d'utilisateur et son mot de passe. Les six autres incidents étaient des attaques d'usurpation d'identité, au cours desquelles un courriel contenant une pièce jointe malicieuse a été envoyé, et un employé a ouvert la pièce jointe.
- Les gestionnaires des employés effectuent un suivi de l'achèvement des cours obligatoires. Si un employé ne termine pas un cours obligatoire, il incombe à son gestionnaire de faire un suivi pour s'assurer qu'il le suit. Nous avons établi que le Bureau du DGIFP n'examine pas les rapports d'achèvement de la formation et ne connaît pas les taux d'achèvement des cours pour les employés de la FPO.
- Le cours obligatoire sur la cybersécurité offert aux employés de la FPO n'a pas de date limite d'achèvement et n'est pas offert régulièrement, par exemple chaque année, conformément aux pratiques exemplaires de l'industrie.

### 4.6.2.2 Aucune formation en cybersécurité n'est offerte aux employés contractuels de la FPO

- LearnON, le système de gestion de l'apprentissage utilisé pour offrir de la formation en ligne aux employés de la FPO, est accessible seulement aux employés à temps plein. Nous avons constaté que les employés contractuels qui travaillent pour la FPO n'ont pas accès à LearnON et ne peuvent donc pas suivre de

**Figure 7 : Formation sur la cybersécurité suivie par le personnel de la FPO, de 2018 à 2022**

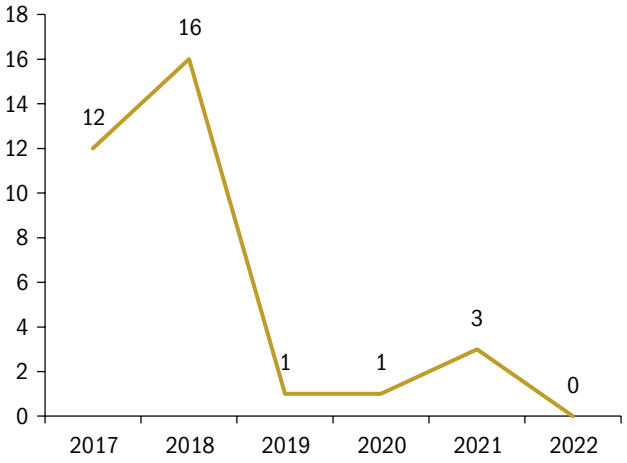
Préparée par le Bureau de la vérificatrice générale de l'Ontario




* Données en date de juillet 2022.

**Figure 8 : Cyberattaques de janvier 2017 à janvier 2022**

Préparée par le Bureau de la vérificatrice générale de l'Ontario



cours, y compris le cours « Principes de base en cybersécurité ».

- Pourtant, les employés contractuels constituent une partie importante de l'effectif de la FPO. En janvier 2022, il y avait environ 7 000 entrepreneurs qui occupaient des postes contractuels à long terme. Bon nombre d'entre eux exerçaient des rôles organisationnels essentiels, comme dans le domaine des ressources humaines et des services sociaux, ou comme consultants en santé et sécurité et agents correctionnels. Ces employés peuvent avoir accès à des données sensibles, comme leurs homologues à temps plein. Le fait de ne pas fournir aux employés contractuels une formation de base sur la cybersécurité ni de les obliger à suivre une telle formation augmente le risque d'incidents de cybersécurité.
- Le Bureau du DGIFP a établi une norme de cybersécurité, mais il n'a pas évalué les risques ni mis en place de contrôles pour protéger les données confidentielles en cas d'utilisation d'appareils personnels. Les bonnes pratiques de l'industrie conseillent de mettre en place des contrôles comme l'interdiction d'utiliser des appareils personnels. Toutefois, le Bureau du DGIFP est incapable d'identifier les employés de la FPO ou de les empêcher d'utiliser des appareils personnels ou de stocker des données gouvernementales confidentielles sur ces appareils.
- Nous avons constaté que les employés à temps plein et contractuels de la FPO peuvent stocker les données de la FPO sur leurs dispositifs USB personnels (stockage externe). De plus, ils peuvent imprimer des documents confidentiels à l'extérieur du réseau de TI de la FPO, comme à la maison.
- Nous avons également constaté que tandis que la FPO dispose d'une politique d'économiseur d'écran automatique obligatoire, environ 1 000 utilisateurs sont exemptés de cette politique et n'ont pas d'économiseur d'écran ou peuvent modifier eux-mêmes les paramètres.

  Cela augmente le risque de sécurité des données puisque des renseignements confidentiels pourraient être vus par une personne non autorisée si l'appareil était laissé sans surveillance, un type de cyberattaque appelé « espionnage par-dessus l'épaule ».

## RECOMMANDATION 7

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;
- offrir une formation en cybersécurité à tout le personnel de la FPO au moins une fois par année;
- 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;
- appliquer une politique d'économiseur d'écran pour tous les utilisateurs.

## RÉPONSE DU MINISTÈRE

Le Ministère souscrit aux recommandations de la vérificatrice générale et continue d'améliorer son programme de formation et de sensibilisation en matière de cybersécurité et s'engage à :

- examiner sa capacité à ouvrir ses cours obligatoires de formation en cybersécurité aux employés contractuels;
- examiner les mécanismes permettant d'assurer l'achèvement des cours obligatoires et mettre en œuvre un processus de recours hiérarchique pour les cours obligatoires incomplets;

- mettre en œuvre une politique exigeant que tous les employés de la FPO suivent une formation sur la cybersécurité chaque année;
- examiner et améliorer les contrôles de TI existants afin de restreindre l'utilisation des appareils personnels et d'empêcher les employés de la FPO qui travaillent à distance de stocker des données sur des appareils autres que ceux de la FPO en documentant les risques associés et en veillant à ce qu'un traitement approprié des risques soit en place;
- examiner les exemptions à la politique existante sur l'économiseur d'écran pour tous les utilisateurs en documentant les risques associés et en veillant à ce qu'un traitement approprié des risques soit en place.

### 4.6.3 Les données de l'Ontario utilisées et stockées dans le secteur parapublic doivent être mieux surveillées par le Bureau du DGIFP

Le secteur parapublic de l'Ontario désigne les organismes qui reçoivent du financement du gouvernement de l'Ontario, mais qui fonctionnent indépendamment de celui-ci, comme les conseils scolaires régionaux, les hôpitaux et les universités. Les entités du secteur parapublic hébergent une grande quantité de renseignements personnels, liés à la santé et délicats, ce qui fait de leurs systèmes de TI une cible attrayante pour les pirates. Les renseignements personnels et sensibles contiennent des données qui peuvent servir à identifier une personne, comme une combinaison de son nom, de son adresse, de ses coordonnées ou de son numéro de téléphone.

De janvier 2018 à juillet 2022, notre Bureau a examiné des articles de presse sur les cyberattaques visant le gouvernement de l'Ontario et le secteur parapublic. Au cours de cette période, le nombre de cyberattaques contre des organismes du secteur parapublic a augmenté. Il y a eu 14 attaques déclarées publiquement, comme l'attaque par rançongiciel contre le Collège des infirmières et infirmiers de l'Ontario, au cours de laquelle des données sensibles et personnelles comme les noms et les dossiers financiers ont été compromises. Une cyberattaque contre le réseau de TI du Conseil scolaire de la région de Durham a entraîné le vol et la fuite du numéro d'immatriculation scolaire de l'Ontario, le nom, la date de naissance, l'adresse et l'emplacement de l'école des élèves.

Le gouvernement de l'Ontario a mis sur pied un groupe d'experts en cybersécurité en octobre 2020. L'objectif du groupe d'experts était de cerner les défis dans le secteur parapublic et de formuler des recommandations pour améliorer la cyberrésilience à l'échelle de la province.

Notre audit a révélé que le Bureau du DGIFP ne fait pas le suivi des cyberattaques touchant le secteur parapublic et n'est pas au courant de celles-ci. Il n'existe pas de fonction centralisée de suivi des incidents ou des atteintes à la cybersécurité. Il s'agit d'une lacune importante, puisque les entités du secteur parapublic comme les conseils scolaires, les collèges et les hôpitaux stockent de grandes quantités de données de la population ontarienne.

À l'heure actuelle, le Centre d'excellence de la Division de la cybersécurité organise des appels mensuels à l'intention de tous les employés du secteur parapublic. Ceux-ci peuvent alors se renseigner sur les nouvelles tendances et pratiques exemplaires en matière de cybersécurité. Toutefois, au cours des cinq dernières années, la Division de la cybersécurité n'a été mobilisée que 15 fois par des entités du secteur parapublic pour effectuer des analyses et des tests de cybersécurité, même si la province compte plus de 200 organisations du secteur parapublic.

#### RECOMMANDATION 8

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.

## RÉPONSE DU MINISTÈRE

Le Ministère souscrit aux recommandations de la vérificatrice générale et se réjouit de l'occasion de tirer parti de ses efforts pour moderniser la cybersécurité dans l'ensemble du secteur public de l'Ontario. Dans le cadre de la Stratégie de cybersécurité de 2023-2026, le Ministère évaluera les possibilités de renforcer son partenariat avec le secteur parapublic au moyen de la Stratégie, ce qui comprend l'établissement d'un cadre de collaboration avec le secteur parapublic afin de partager des rapports détaillés sur les incidents de cybersécurité et de communiquer la façon de corriger les faiblesses dans le cadre de sa stratégie de cybersécurité à l'avenir.

### 4.6.4 Les risques de cybersécurité des systèmes de TI des fournisseurs ne sont pas évalués

En août 2022, le Bureau du DGIFP a eu recours à 140 fournisseurs de TI pour gérer, au nom de la FPO, les services et systèmes de TI qui sont essentiels à la continuité des programmes et des opérations du gouvernement. Nous avons demandé une liste des rapports d'assurance reçus et examinés par le Bureau du DGIFP au sujet de ces fournisseurs de services. Le Bureau du DGIFP n'a pas été en mesure de nous fournir des rapports de contrôle de l'organisation de services, car il n'obtient ni n'examine les rapports d'assurance de tiers pour cerner les vulnérabilités en matière de cybersécurité et les faiblesses des TI. Par conséquent, il n'est pas en mesure d'évaluer l'impact potentiel sur ses activités commerciales et ne connaît pas les risques auxquels il expose les Ontariens. La production de rapports d'assurance par des tiers représente une source essentielle d'information pour déterminer les risques et les faiblesses des TI, y compris les risques liés à la cybersécurité.

De plus, nous avons remarqué que le Bureau du DGIFP ignorait si l'un des fournisseurs de services retenus par les groupements de TI stockait les données des Ontariens à l'extérieur du Canada, ce qui contreviendrait aux exigences provinciales en matière de protection des renseignements personnels et de sécurité des données liées à la collecte, à la conservation et à l'élimination de renseignements de nature délicate.

## RECOMMANDATION 9

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 stockés à l'extérieur de l'Ontario.

## RÉPONSE DU MINISTÈRE

Le Ministère souscrit aux recommandations de la vérificatrice générale et reconnaît l'importance de cerner les risques auxquels les données du gouvernement de l'Ontario peuvent être exposées. Aujourd'hui, les évaluations de sécurité sont effectuées dans le cadre des pratiques de passation de marchés avec des fournisseurs de la FPO, où les modalités de sécurité sont reflétées dans les contrats afin d'assurer la protection continue des données du gouvernement et de respecter les exigences de résidence des données.

À cet égard, le Ministère élabore une stratégie de cybersécurité actualisée et entend y intégrer la gestion des fournisseurs. La stratégie comprendra un engagement à :

- établir des processus pour rendre obligatoire la réception des rapports d'assurance de tiers;
- examiner les faiblesses relevées dans les rapports d'assurance de tiers et leur incidence sur les opérations de la FPO et prendre des mesures correctives pour atténuer le risque;
- collaborer avec les ministères et les groupements de TI pour repérer les fournisseurs qui stockent des données à l'extérieur du Canada et prendre des mesures correctives pour atténuer le risque.

## 4.7 L'inventaire des systèmes de TI du gouvernement de l'Ontario est incomplet et inexact

Il importe que toute organisation dispose d'un inventaire complet et à jour des biens de TI pour s'assurer que ses biens de TI sont comptabilisés, tenus à jour et éliminés de façon appropriée. Les inventaires de biens servent également à recenser les biens de TI vieillissants et à quel moment des contrôles de sécurité des TI sont nécessaires.

Comme le Bureau du DGIFP est responsable de l'achat de tous les biens de TI du gouvernement de l'Ontario, il utilise la base de données de gestion des configurations (BDGC) pour suivre et surveiller tous les biens de TI. La BDGC contient de l'information sur les systèmes de TI, comme Paiements de transfert Ontario et le Système automatisé de gestion de l'aide sociale dont les Ontariens se servent pour demander et recevoir de l'aide sociale. La BDGC comprend habituellement des renseignements tels que le nom du système de TI, sa criticalité, le propriétaire (personne responsable), le ministère associé (utilisateur principal) et le groupement de TI responsable de ses services.

Nous avons obtenu un extrait des données de la BDGC pour tous les systèmes de TI. Sur un total de 1 212 systèmes de TI faisant l'objet d'un suivi et d'une surveillance, nous avons constaté que même si l'inventaire fait l'objet d'un suivi, la base de données est incomplète. Elle ne contient pas tous les renseignements pertinents et essentiels sur chaque système de TI. La **figure 9** présente la liste des principaux attributs de données manquants dans la BDGC.

De plus, nous avons constaté que le processus actuellement en place pour examiner les lacunes de la BDGC ne contient pas d'examens rigoureux, réguliers et uniformes fondés sur des critères afin de vérifier que l'information stockée est exacte, complète et à jour. Bien que l'équipe de gestion des biens du Bureau du DGIFP procède à des examens informels pour repérer

**Figure 9 : Attributs de données critiques non énumérés dans la base de données de gestion des configurations**

Préparée par le Bureau de la vérificatrice générale de l'Ontario

| Attribut de données | Description | Nombre de systèmes de TI comportant des attributs de données manquants |
|---|---|---|
| Technologie de stockage des données | Endroit où les données sont stockées (centre de traitement de l'information de la FPO ou nuage) | 179 |
| Frais d'hébergement | Coûts annuels d'hébergement dans tous les environnements | 145 |
| Soutient la fonction législative | Indique si le système de TI soutient une fonction législative ou de conformité, comme l'inspection, l'enquête et l'application de la loi | 141 |
| Frais de licence | Droits de licence ou frais non liés à l'hébergement | 115 |
| Évaluation de l'impact sur la protection de la vie privée | Indique si une évaluation de l'impact sur la protection de la vie privée a été effectuée | 51 |
| Évaluation des menaces et des risques | Indique si une évaluation de la menace et des risques a été effectuée | 47 |

les données périmées et manquantes dans la BDGC, les examens ne sont pas effectués selon une fréquence ou des critères définis. Par conséquent, le Bureau du DGIFP ne dispose pas d'un relevé exact de l'âge des biens.

En octobre 2021, la Division de la vérification interne de l'Ontario a publié un rapport d'audit concernant les systèmes de TI désuets dans la FPO. Ce rapport a conclu que 23,5 % de tous les systèmes de TI de la FPO ont vieilli et, par conséquent, ne bénéficient plus du soutien des fournisseurs. Comme cet audit récent a été effectué par la Division de la vérification interne, nous avons exclu de notre mandat une évaluation de l'âge des systèmes de TI dans la FPO. Le Bureau du DGIFP était en train de donner suite au rapport et à la recommandation de la Division de la vérification interne. Il avait pour objectif de mettre complètement à jour l'inventaire des biens de TI d'ici le début de 2023.

## RECOMMANDATION 10

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.

## RÉPONSE DU MINISTÈRE

Le Ministère souscrit à cette recommandation et s'engage à améliorer l'exactitude et l'exhaustivité de l'inventaire des systèmes de TI et à repérer plus efficacement les systèmes vieillissants. À cet égard, la Division des services technologiques d'infrastructure collaborera avec la Division de la stratégie en matière de technologie pour la FPO et les groupements pour :

- améliorer le processus existant pour son personnel afin que la base de données de gestion de la configuration soit mise à jour au moyen d'un ensemble défini de critères;
- examiner et remplir les champs obligatoires dans la base de données de gestion de la configuration pour les systèmes de TI;
- élaborer un processus d'examen annuel systématique ou chaque fois qu'un nouveau système est intégré, pour permettre aux groupements et aux propriétaires des systèmes de TI de repérer les données manquantes, de les mettre à jour et de confirmer leur exhaustivité.

### 4.7.1 Les licences de logiciels ne sont pas toutes gérées ou comptabilisées

Un registre complet et exact de toutes les licences de logiciels et des logiciels installés est utile à une organisation pour obtenir, gérer et résilier efficacement les licences au besoin. Cela fait partie d'un processus efficace de gestion des biens qui permet d'éviter les coûts de toute licence de logiciel excédentaire inutilisée, de gérer les licences nécessaires pour poursuivre les opérations, et de détecter et éviter l'utilisation de logiciels piratés.

Nous avons remarqué que le Bureau du DGIFP ne dispose pas d'un processus pour gérer de façon efficace et efficiente les licences de logiciels pour tous les systèmes des fournisseurs de TI. À l'heure actuelle, les licences de logiciels sont gérées au moyen d'un système de suivi central appelé Snow. Au 31 août 2022, le Bureau du DGIFP n'avait inscrit que trois fournisseurs (Oracle, IBM et Microsoft) pour assurer le suivi des licences et de l'utilisation des logiciels. Toutefois, il ne fait pas le suivi de l'utilisation des 137 autres fournisseurs de TI pour lesquels il a obtenu une licence de logiciel. Par conséquent, le Bureau du DGIFP n'a pas présentement d'inventaire d'autres licences de logiciels installées sur les postes de travail des employés ni de leurs coûts et utilisations connexes.

Nous avons également constaté qu'il n'existe aucun processus au Bureau du DGIFP pour établir un rapprochement approprié entre le nombre de licences achetées et les frais payés aux fournisseurs pour ces licences. Le Bureau du DGIFP s'en remet aux fournisseurs pour qu'ils effectuent leurs propres audits du nombre de licences achetées. Il ne sait donc pas et n'accomplit aucun travail pour déterminer s'il existe des situations de sous-paiement ou de trop-payé éventuels des fournisseurs pour les licences de logiciels.

## RECOMMANDATION 11

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.

## RÉPONSE DU MINISTÈRE

Le Ministère souscrit à cette recommandation et s'engage à :

- continuer d'élargir l'utilisation d'un outil de gestion des actifs logiciels pour y intégrer d'autres fournisseurs de logiciels clés;
- veiller à ce que des processus soient en place pour vérifier et valider les droits aux licences et l'exactitude des paiements versés aux fournisseurs, et aider à la vérification des logiciels installés au besoin.

## 4.8 Le Bureau du DGIFP n'a pas exercé une diligence raisonnable suffisante lors de l'embauche de consultants en TI

Le Bureau du DGIFP embauche tous les consultants contractuels en TI par l'entremise d'un seul fournisseur de services de recrutement, Flextrack. Il a versé environ 16 millions de dollars à Flextrack de 2020-2021 à 2021-2022. En outre, les ministères et les groupements ont versé à Flextrack environ 146 millions de dollars au cours de cette période pour faire appel à des entrepreneurs dans des postes de TI et dans d'autres postes.

Nous avons sélectionné un échantillon de 30 consultants en TI sur un total de 244 consultants au service du Bureau du DGIFP au cours de la période du 1er avril 2021 à avril 2023. Pour chaque employé, nous avons examiné la justification commerciale de l'embauche d'un employé contractuel, les évaluations des capacités internes, les notes d'entrevue et la feuille d'évaluation du pointage, ainsi que les approbations des feuilles de temps par les superviseurs. Les feuilles de temps approuvées sont envoyées à Flextrack. Selon la directive sur l'approvisionnement de la FPO, avant de demander des services externes de consultation, une organisation doit d'abord tenir compte de ses ressources humaines internes et justifier l'embauche d'employés occasionnels. L'évaluation des capacités internes comprend une analyse coûts-avantages pour évaluer le coût relatif de l'embauche d'un consultant par rapport au recrutement d'un employé équivalent temps plein pour le poste.

### Les évaluations des capacités n'ont pas été effectuées avant l'embauche de consultants, ce qui a entraîné des coûts plus élevés

Nous avons examiné les formulaires de demande d'embauche et les notes d'information soumis par le Bureau du DGIFP au Secrétariat du Conseil du Trésor pour 30 consultants en TI. Le Bureau du DGIFP n'a pas effectué d'évaluation des capacités internes pour 28 des 30 rôles. En ce qui concerne les deux rôles ayant fait l'objet d'une évaluation, nous avons calculé que l'embauche d'un employé équivalent temps plein

coûtait moins cher annuellement que celle d'un consultant. Par exemple, le coût d'embauche d'un consultant pour le poste de spécialiste en assurance de la qualité des TI était d'environ 132 000 $ comparativement à environ 86 000 $ pour le salaire annuel de l'employé à temps plein. Le Bureau du DGIFP nous a mentionné qu'il avait embauché un consultant parce qu'il n'y avait pas de ressources à temps plein disponibles à l'interne.

Nous avons également constaté que le Bureau du DGIFP n'avait pas effectué d'évaluation pour déterminer si l'embauche d'un employé à temps plein était plus rentable que l'embauche d'un consultant. Dans un autre exemple, le Bureau du DGIFP a fini par embaucher deux consultants en TI pour le rôle de développeur en TI. Ces contrats ont coûté environ 403 000 $ pour un an pour les deux. L'évaluation a permis de constater que le coût d'embauche de deux employés à temps plein était d'environ 248 000 $, en excluant environ 22 % du salaire brut alloué aux avantages sociaux.

Nous avons également constaté que les évaluations du rendement des consultants n'avaient pas été examinées. Le rendement des consultants n'avait aucune incidence sur la question de savoir s'ils obtiendraient ou non un autre contrat.

## Les consultants ont reçu une rémunération supérieure au taux recommandé

Le manuel des services de placement des employés de la FPO créé par le Secrétariat du Conseil du Trésor recommande que les consultants soient rémunérés conformément au tableau de référence sur les taux du marché conçu pour le manuel. Les taux de rémunération sont établis en fonction d'un certain nombre de facteurs, comme le titre du poste et les responsabilités.

Nous avons comparé le taux de rémunération quotidien recommandé dans le tableau de référence sur les taux du marché aux taux réels payés aux 244 consultants en TI embauchés par le Bureau du DGIFP depuis le 1er avril 2021. Nous avons constaté que 25 de ces employés avaient obtenu des taux de rémunération supérieurs au niveau recommandé. Le Bureau du DGIFP n'a fourni aucune justification du taux de rémunération plus élevé. De plus, 25 consultants sur un total de 244 ont reçu en moyenne 86 $ de plus que le taux quotidien recommandé. Par exemple, un consultant en TI touchait 1 199 $ par jour, même si le taux quotidien recommandé s'établissait à 967 $, soit une différence de 232 $. Cela représente un coût additionnel total de 51 736 $ pour la durée du contrat de sept mois et demi. Au total, pour ces 25 entrepreneurs, le Bureau du DGIFP a versé environ 470 000 $ de plus que ce que recommandait le Secrétariat du Conseil du Trésor.

## Le processus d'évaluation des entrevues doit être amélioré

L'évaluation d'entrevue est un aspect essentiel du processus de sélection des consultants, car elle permet à l'évaluateur d'apprécier le candidat en fonction des critères de sélection. Les candidats dont le curriculum vitae obtient une note supérieure à 70 % se voient accorder une entrevue.

Nous avons toutefois constaté qu'il n'est pas nécessaire qu'un nombre minimal de candidats soient interviewés à l'étape de l'entrevue. Cela a donné lieu à des scénarios dans lesquels un seul candidat a été interviewé pour le poste contractuel en TI, comme ce fut le cas pour 4 des 30 consultants de notre échantillon. Nous avons également constaté que ce poste contractuel est un poste très convoité dans les organisations et que de nombreuses candidatures sont habituellement envoyées lorsqu'un poste est affiché.

Selon le manuel des services de placement des employés, les concurrents pour les postes contractuels doivent être interrogés par au moins trois évaluateurs équivalents temps plein. Pour 8 des 30 employés de notre échantillon, l'entrevue a été effectuée par seulement 2 évaluateurs.

Enfin, nous avons constaté que 21 des 30 intervieweurs (70 %) n'avaient pas saisi de notes ni de commentaires d'entrevue dans leur feuille de notation ou dans le SGF. Il n'est pas nécessaire de saisir des notes d'entrevue dans le système de TI du SGF. Nous avons également constaté que 6 des 30 intervieweurs (20 %) ont fourni des notes d'entrevue très limitées.

## RECOMMANDATION 12

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.

## RÉPONSE DU MINISTÈRE

Le Ministère tient à remercier la vérificatrice générale et son équipe, souscrit à ses recommandations et s'engage à améliorer ses pratiques et à accroître la transparence et la responsabilisation.

À cet égard, le Ministère s'engage à :

- mettre en œuvre une approche uniforme pour permettre un examen des options en matière de capacité et de ressources avant de retenir les services de consultants en TI. Les consultants en TI seront embauchés conformément aux recommandations, selon les taux du marché prévus par le Secrétariat du Conseil du Trésor dans la mesure du possible;
- veiller à ce que le niveau d'approbation approprié soit obtenu et documenté pour soutenir les cas exceptionnels;
- examiner les règles, les contrôles et les pratiques exemplaires à l'appui du processus d'entrevue et de sélection lors de l'embauche de consultants en TI. Plus précisément, on veillera à ce qu'au moins deux candidats par poste soient interviewés par au moins trois évaluateurs et que les notes d'entrevue soient officiellement documentées et conservées dans le système de TI.

## 4.9 Les cibles de résolution des incidents de TI sont désuètes

Le Bureau du DGIFP a établi un processus de classification des incidents de TI qui permet de distinguer la priorité d'un incident, allant de ceux dont l'incidence est la plus importante (« critique ») à ceux dont l'incidence est la moins importante (« faible »). Le Bureau du DGIFP considère comme critiques les incidents qui pourraient entraîner une perte de données sur les clients, porter atteinte à la sécurité ou empêcher des clients d'accéder aux pages Web qui leur sont destinées.

Notre Bureau a examiné les données sur les incidents de TI d'avril 2017 à mars 2022 et a constaté qu'au total, 2 057 917 incidents se sont produits pour tous les systèmes de TI de la FPO. Ces incidents ont été consignés dans Remedy, le système de TI utilisé par différents groupements de TI de la FPO pour visualiser et résoudre les incidents de TI. Lorsqu'un incident de TI est résolu dans le délai défini par l'entente de niveau de service applicable, l'option « met » (exigence satisfaite) est sélectionnée dans le système de TI Remedy. S'il est résolu en dehors du délai prévu dans l'entente sur les niveaux de service, l'option « missed » (exigence non satisfaite) est sélectionnée. La **figure 10** présente la répartition des 2 057 917 incidents par niveau de priorité ainsi que le pourcentage d'incidents de TI qui ont respecté le délai de résolution convenu. Nous avons noté 803 incidents de TI critiques prioritaires.

### 4.9.1 Les cibles de conformité du Bureau du DGIFP pour résoudre les incidents de TI sont désuètes

Le Bureau du DGIFP a une cible de conformité de 90 % pour tous les billets de prestation de services

**Figure 10 : Nombre d'incidents de TI par niveau de priorité et pourcentage de cas résolus d'avril 2017 à mars 2022**

Préparée par le Bureau de la vérificatrice générale de l'Ontario

| Niveau de priorité | Nombre de résultats insatisfaisants | % de résolution (Bureau du DGIFP)[1] | % de résolution (BVGO)[2] | % de résolution (BVGO)[3] |
|---|---|---|---|---|
| Critique | 803 | 73,2 | 66,5 | 47,8 |
| Élevé | 4 215 | 86,8 | 85,8 | 75,8 |
| Moyen | 905 316 | 93,4 | 93,4 | 83,1 |
| Faible | 1 147 583 | 96,6 | 96,6 | 92,5 |
| **Total** | **2 057 917** | **95,2** | **85,6** | **74,8** |

1. Pourcentage de résolution calculé par le système de gestion des incidents de TI du Bureau du DGIFP (Remedy)
2. Pourcentage de résolution calculé par le BVGO en comparant le moment où l'incident de TI a été signalé au moment où il a été résolu
3. Pourcentage de résolution calculé par le BVGO en comparant le moment où l'incident de TI a été signalé au moment où il a été résolu, en excluant le temps de mise en attente

liés aux incidents de TI en fonction des délais cibles pour les systèmes essentiels aux opérations, essentiels à la mission et de soutien opérationnel. La **figure 11** indique les délais de résolution visés pour les incidents de TI selon la classification des systèmes de TI.

La cible de conformité de 90 % du Bureau du DGIFP a été établie en 2016 et n'a pas été réévaluée depuis. De plus, les objectifs de service du Bureau du DGIFP sont moins élevés que les pratiques exemplaires de l'industrie. Par exemple, un incident de TI dont le statut est critique devrait être réglé dans un délai de 1 à 2 heures, alors que la cible du Bureau du DGIFP est de 4,5 heures.

### 4.9.2 Les objectifs de résolution des incidents de TI n'ont pas été atteints

À l'aide de l'analyse des données, nous avons réévalué les 2 057 917 incidents de TI pour déterminer s'ils avaient été résolus conformément à la cible de conformité de 90 % définie par le Bureau du DGIFP et dans les délais précisés dans les ententes sur les niveaux de service. La **figure 10** présente une ventilation des incidents par niveau de priorité et pourcentage de résolution signalés par le Bureau du DGIFP et le Bureau de la vérificatrice générale de l'Ontario (BVGO). Nous avons constaté que le Bureau du DGIFP avait déclaré une conformité globale de 95 % pour tous les incidents de TI au cours des cinq dernières années. Toutefois, d'après notre examen et notre analyse, la conformité globale était de 85 % pour tous les incidents de TI. Cet écart de 10 % est attribuable au fait que le Bureau du DGIFP calcule le taux de conformité en utilisant le temps écoulé, soit le temps consacré par le technicien pour résoudre le billet d'incident, alors que pour notre calcul, nous avons comparé le temps écoulé entre le moment de la création du billet d'incident et la fermeture du

**Figure 11 : Délais de résolution cibles pour les types d'incidents de TI**

Préparée par le Bureau de la vérificatrice générale de l'Ontario

| Classification des systèmes de TI | Incident à priorité critique | Incident à priorité élevée | Incident à priorité moyenne |
|---|---|---|---|
| Essentiel à la mission[1] | 4,5 heures | 1 jour | 5 jours |
| Essentiel aux activités[2] | 4,5 heures | 1 jour | 10 jours |
| Soutien opérationnel[3] | Aucune limite de temps | 1 jour | 15 jours |

1. **Essentiel à la mission** : utilisé uniquement pour les solutions dans les cas où une défaillance peut i) nuire à la santé des Ontariens ou ii) mettre en danger la vie des Ontariens ou créer des risques pour la sécurité ou iii) réduire la capacité de production de revenus du gouvernement ou iv) empêcher les paiements essentiels.
2. **Essentiel aux activités** : utilisé uniquement lorsque la solution i) appuie les priorités du gouvernement ou ii) démontre un lien direct avec les systèmes, les applications et l'infrastructure essentiels à la mission ou iii) démontre que la défaillance menacera les projets essentiels à la mission ou iv) soutient le rôle d'intendance du gouvernement.
3. **Soutien opérationnel** : utilisé uniquement lorsque les solutions sont essentielles au fonctionnement d'une unité opérationnelle ou d'un service, mais ne sont pas directement essentielles à la prestation d'un programme ou d'un service public. Sa portée se limite à une unité opérationnelle plus petite que celle des services essentiels aux activités.

billet. Nous avons également constaté que le taux de conformité des incidents de TI ayant les répercussions les plus importantes (« critiques ») était de 66 %.

Nous avons également constaté que 95 % des cas de conformité signalés par le Bureau du DGIFP comprennent le temps « en attente », c'est-à-dire le temps pendant lequel les demandes d'incident de TI sont mises en attente, car ils sont en attente d'une confirmation de l'employé ou des utilisateurs touchés pour valider si l'incident de TI a été résolu. Nous avons remarqué que sur les 2 057 917 incidents de TI, 418 145 (20 %) avaient été mis en attente avant d'être finalement résolus. Nous avons également remarqué qu'il n'y avait pas de processus en place pour vérifier que les 20 % des demandes nécessitent réellement un temps d'attente, car le système ne saisit pas ce niveau de détail dans les journaux de vérification. Nous avons effectué une autre analyse qui excluait le temps d'attente et constaté que la conformité globale des incidents de TI baissait à 75 %. Voir la **figure 10**.

## RECOMMANDATION 13

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.

## RÉPONSE DU MINISTÈRE

Le Ministère souscrit à cette recommandation et s'engage à :

- déterminer les améliorations à apporter aux cibles de prestation des services pour les systèmes essentiels et les incidents hautement prioritaires, en fonction des résultats des analyses de l'industrie;
- examiner et mettre à jour le temps de résolution des incidents pour s'assurer que les paramètres et les rapports sont conformes aux pratiques exemplaires de l'industrie;
- mettre en œuvre tout changement apporté aux cibles actuelles de prestation des services pour l'exercice 2025-2026.

# Annexe 1 : Glossaire des acronymes

Préparée par le Bureau de la vérificatrice générale de l'Ontario

| Terme/acronyme | Définition |
|---|---|
| BAE | Bureau de l'avocat des enfants |
| BDGC | Base de données de gestion des configurations – système de TI utilisé pour effectuer le suivi des renseignements liés aux biens de TI, comme le nom, l'utilisateur et la date de déploiement. |
| CAPO | Commission d'arbitrage de la police de l'Ontario |
| DGI | Directeur général de l'information |
| DGIFP | Bureau du directeur général de l'information pour la fonction publique |
| DGSI | Directeur général de la sécurité de l'information |
| DNMRNF | Ministère du Développement du Nord, des Mines, des Richesses naturelles et des Forêts |
| DT | Directeur de la technologie |
| EIPVP | Évaluation de l'impact sur la protection de la vie privée |
| EMR | Évaluation des menaces et des risques. |
| EQTI | Entreprises qualifiées en technologies de l'information |
| ETP | Équivalent temps plein |
| FPO | Fonction publique de l'Ontario |
| GGR | Gestion globale des risques |
| GISG | Groupement d'intégration des services gouvernementaux |
| GOC | Groupement pour les organismes centraux |
| GSS | Groupement des services de santé |
| INF | Ministère de l'Infrastructure |
| IRP | International Registration Plan |
| IUVU | Immatriculation d'utilisateur de véhicule utilitaire – système informatique automatisé utilisé pour stocker des renseignements sur les transporteurs de gros véhicules |
| MTO | Ministère des Transports |
| PRIO | Système de gestion des permis et de l'immatriculation pour le plan d'immatriculation international et les véhicules ou charges de dimensions/poids exceptionnels |
| PTF | Prestation en matière de technologie pour la FPO |
| RAP | Reprise après sinistre |
| SGF | Système de gestion des fournisseurs – traite et tient à jour les documents relatifs aux fournisseurs |
| STF | Stratégie en matière de technologie pour la FPO |
| STI | Services technologiques d'infrastructure |
| TI | Technologie de l'information |

## Annexe 2 : Personnes supervisant les huit groupements de TI, en date de septembre 2022

| Groupement | Directeur général de l'information ou sous-ministre adjoint | Sous-ministre | Ministre |
|---|---|---|---|
| Services à la collectivité | Soussan Tabari | Nancy Naylor | Stephen Lecce |
| Services sociaux et services à l'enfance et à la jeunesse | Alex Coleman | Denise Allyson Cole | Merrilee Fullertone |
| Services de santé | Angela Copeland | Catherine Zahn | Christine Elliott |
| Services technologiques de la justice | Catherine Emile | David Corbett | Doug Downey |
| Terres et ressources | Rocco Passero | Monique Rolf von den Baumen Clark | Greg Rickford |
| Travail et transports | Roman Corpuz | Douglas Jones | Caroline Mulroney |
| Organismes centraux | Liz Mackenzie | Deborah Richardson | Prabmeet Sarkaria |
| Intégration des services gouvernementaux | Manish Agarwal | Renu Kulendran | Kaleed Rasheed |

## Annexe 3 : Responsabilités de haut niveau du Bureau du directeur général de l'information pour la fonction publique par rapport aux groupements

Préparée par le Bureau de la vérificatrice générale de l'Ontario

| Services | DGIFP | Groupements |
|---|---|---|
| Cybersécurité | Effectuer des analyses de sécurité et réagir aux incidents pour :<br>1. Évaluation des menaces et des risques<br>2. Analyses de cybersécurité<br>3. Analyses de vulnérabilité<br>4. Intervention en cas d'incident | Identifier les systèmes de TI applicables et demander des cyberanalyses et des évaluations |
| Gestion des biens | Les STI gèrent, suivent et distribuent des biens matériels comme des ordinateurs portables et des serveurs. | Demander un nouveau matériel et collaborer avec les STI pour obtenir les biens requis |
| Prestation des services de TI | Établir des objectifs et des cibles de conformité pour la prestation des services pour l'ensemble de la FPO | Les équipes de gestion des incidents travaillent au sein du groupe et font rapport des mesures de rendement au Bureau du DGIFP. |
| Gestion des fournisseurs | Gérer les contrats intégrés des fournisseurs comme les contrats avec Compucom et TELUS | Faire appel aux fournisseurs avec l'aide de leurs propres gestionnaires de contrat |

# Annexe 4 : Taux de rémunération journalier les plus élevés recommandés pour les entrepreneurs en TI, établis par le Secrétariat du Conseil du Trésor

Préparée par le Bureau de la vérificatrice générale de l'Ontario

| Rôle | Tarif journalier recommandé ($) |
|---|---|
| Chef des programmes | 1 015,00 |
| Chef/responsable de projet | 983,00 |
| Architecte des applications | 967,00 |
| Architecte de la technologie | 967,00 |
| Spécialiste de l'évaluation de l'impact sur la protection de la vie privée (EIPVP) | 966,00 |
| Conseiller en solutions d'automatisation | 954,00 |
| Architecte des systèmes opérationnels | 954,00 |
| Concepteur de solutions | 940,00 |
| Ingénieur en nuage/DevFPO | 936,00 |
| Spécialiste des renseignements opérationnels | 925,00 |

# Annexe 5 : Objectif et critères d'audit

Préparée par le Bureau de la vérificatrice générale de l'Ontario

## Objectif de l'audit

Cet audit vise à déterminer si le Bureau du directeur général de l'information pour la fonction publique a mis en place des systèmes et une gouvernance de TI efficaces pour assurer ce qui suit :

| | |
|---|---|
| 1. | Un cadre de gouvernance est mis en œuvre et englobe une stratégie globale de TI qui démontre une surveillance efficace des fonctions de TI afin de fournir des services de TI à la fonction publique de l'Ontario et aux Ontariens de façon efficiente et efficace. |
| 2. | Les opérations et systèmes de TI sont surveillés de manière efficace conformément aux mesures de rendement établies, et des mesures correctives sont prises après examen. |
| 3. | Les données et les biens de TI des Ontariens, y compris le matériel et les logiciels, sont sécurisés, fiables et protégés contre les cyberattaques. |
| 4. | Les ressources de TI, y compris les fournisseurs dans ce domaine, sont acquises conformément aux exigences législatives, réglementaires et contractuelles, en tenant dûment compte de l'économie. |

## Critères d'audit

| | |
|---|---|
| 1. | Un cadre de gouvernance efficace avec une supervision adéquate des opérations, de la stratégie et de la responsabilisation en matière de TI et des attributions claires sont en place pour atteindre les buts et objectifs stratégiques en matière de TI. |
| 2. | Des mesures et des cibles appropriées de rendement en matière de TI ont été définies et approuvées. Un processus de surveillance est en place pour évaluer le rendement et les services de TI fournis à la fonction publique de l'Ontario et pour faire rapport régulièrement. |
| 3. | Des systèmes et des contrôles de cybersécurité en TI sont en place pour détecter, prévenir et atténuer les anomalies et les menaces aux activités de la FPO en temps opportun, notamment en protégeant les renseignements personnels identificatoires et les données sensibles de la FPO protégés par la loi. |
| 4. | Des processus sont en place pour s'assurer que l'approvisionnement est géré de façon économique conformément aux règlements applicables et que le rendement des fournisseurs fait l'objet d'une surveillance pour assurer la livraison satisfaisante des biens et services. |

# Annexe 6 : Liste des organismes de la FPO et de la Couronne et des services publics connexes touchés par une interruption de service chez Rogers le 8 juillet 2022

Préparée par le Bureau de la vérificatrice générale de l'Ontario

| Service/organisation | Description | Incidence |
|---|---|---|
| AgriSuite GoCloud | Système de TI utilisé par les agriculteurs et les consultants agricoles. | Le site Web n'était pas disponible. |
| Brigade des bénévoles de l'Ontario | Demande de renseignements auprès du centre de contact pour la brigade des bénévoles de l'Ontario. | La ligne téléphonique n'était pas disponible. |
| Cabinet du premier ministre | Pour communiquer avec le premier ministre. | La ligne téléphonique n'était pas disponible. |
| Centre de services à la clientèle de la Commission du Régime de retraite de l'Ontario | Centre de contact utilisé pour les demandes de renseignements généraux. | Le temps d'attente était plus long que la normale pour un centre d'appels. |
| Commission d'arbitrage de la police de l'Ontario (CAPO) | Le site Web de la CAPO permet d'effectuer des recherches dans les conventions collectives, les différends en matière d'intérêts et de droits, et le contenu connexe concernant le processus de conciliation et d'arbitrage en vertu de la *Loi sur les services policiers*. | Le site Web n'était pas disponible. |
| Dossiers en ligne des transporteurs du MTO | Portail public pour accéder en ligne à leur dossier d'IUVU. | Le site Web n'était pas disponible. |
| Étude des dossiers médicaux des conducteurs (EDMC) | Le programme d'EDMC examine les conducteurs qui ont certains problèmes médicaux ainsi que les évaluations de l'aptitude à conduire en fonction des politiques du MTO prévues par la loi. | Le site Web n'était pas disponible. |
| Hôpitaux | De nombreux hôpitaux ont été touchés par la panne. Les hôpitaux ont eu de la difficulté à joindre le personnel qui était à la maison, ce qui a entraîné des temps d'attente plus longs dans les hôpitaux. De plus, les hôpitaux ont de la difficulté à communiquer avec les membres de la famille et les partenaires du système de santé (comme les établissements de soins de longue durée). | Le site Web et les communications téléphoniques n'étaient pas disponibles |
| iCorridor du MTO | iCorridor est un outil de visualisation des données cartographiques et de partage de l'information visant à mieux comprendre l'information historique, en temps réel et prévisionnelle dans la planification des transports et de l'utilisation des terres. | Le site Web n'était pas disponible. |
| Localisation des bureaux de santé publique | Recherche géographique du bureau de santé qui régit la région de l'utilisateur. | Le site Web n'était pas disponible. |

| Service/organisation | Description | Incidence |
|---|---|---|
| MesPrestations | Les bénéficiaires de l'aide sociale sont incapables d'accéder à leur compte. | Le site Web n'était pas disponible. |
| Metrolinx et GO Transit | Services de transport public dans la région du grand Toronto | Certains établissements et tarifs ne pouvaient pas être achetés par carte de débit ou de crédit. Les billets électroniques n'étaient pas disponibles. |
| Portail d'inscription pour services aux enfants | Interagir avec le Bureau de l'avocat des enfants pour accéder aux renseignements sur les cas et soumettre des renseignements sur le système de TI relatif aux enfants (service de base). | Le site Web n'était pas disponible. |
| Portail de consultation technique du MTO | Il fournit un système de TI utilisé par le MTO et son fournisseur. | Le site Web n'était pas disponible. |
| Procureur général | Pour communiquer avec le ministère du Procureur général. | La ligne téléphonique n'était pas disponible. |
| Site Web 511 du ministère des Transports | Accès à l'information routière | Le site Web n'était pas disponible. |
| Société des loteries et des jeux de l'Ontario | Services de jeux pour le public ontarien | Le public ne pouvait pas acheter de billets de loterie. |
| Système de gestion des permis et de l'immatriculation pour le plan d'immatriculation international et les véhicules ou charges de dimensions/ poids exceptionnels (PRIO) | Permis et immatriculation des transporteurs commerciaux basés en Ontario pour les voyages intergouvernementaux au Canada, aux États-Unis et au Mexique | Le site Web n'était pas disponible. |
| Toronto District School Board | Étudiants et membres du personnel participant à des séances estivales d'apprentissage à distance. | L'apprentissage en ligne n'était pas disponible; les participants ont dû passer à un apprentissage asynchrone. |
| Tribunaux décisionnels Ontario (Commission de la location immobilière) | Ligne téléphonique pour parler à un agent du service à la clientèle. | La ligne téléphonique n'était pas disponible. |

Bureau de la vérificatrice générale de l'Ontario

20, rue Dundas Ouest, bureau 1530
Toronto (Ontario)
M5G 2C2

www.auditor.on.ca

ISBN 978-1-4868-6519-2 (PDF)