



## Systèmes de technologie de l'information (TI) et cybersécurité à l'agence Metrolinx

### Audit de l'optimisation des ressources 2020

#### Pourquoi nous avons effectué cet audit

- Les systèmes de technologie de l'information (TI) de Metrolinx jouent un rôle essentiel dans la gestion courante des opérations de transport en commun, qui se sont soldées par plus de 76 millions de déplacements d'usagers en 2019-2020.
- Compte tenu de l'évolution de la technologie dans l'industrie des transports, la cybersécurité est une préoccupation croissante en raison de l'augmentation des cyberattaques au fil de la croissance de la technologie.

#### Pourquoi cet audit est-il important?

- Les interruptions causées par des problèmes de TI peuvent affecter l'expérience des clients en ce qui concerne les retards et les annulations de trains, et le paiement des tarifs, et réduire les revenus de la province.
- La cybersécurité est une mesure essentielle pour protéger Metrolinx contre les cyberattaques, les atteintes à la vie privée et l'accès non autorisé à l'infrastructure de TI.

#### Nos constatations

- Les activités essentielles de transport en commun ont fait l'objet d'incidents de TI, comme des difficultés de connexion au réseau, des défaillances des systèmes et des anomalies dans les logiciels et le matériel, ce qui s'est traduit par des retards et des annulations de déplacements. Nous avons constaté qu'entre janvier 2015 et janvier 2020, près de 4 500 retards et annulations de services du Réseau GO et d'UP Express ont été enregistrés à la suite de problème de logiciel et de matériel de TI.
- Bien que Metrolinx dispose de la technologie et des données nécessaires pour rembourser automatiquement les usagers admissibles au Programme de garantie de service, elle ne le fait pas. Au cours des cinq dernières années, sur les 4 500 retards et annulations de trains attribuables à des incidents de TI, seulement 23 % des clients admissibles ont présenté une demande au Programme de garantie de service pour un remboursement total d'environ 450 000 \$, et environ 2,2 millions de dollars de remboursements applicables n'ont pas été réclamés.
- Le système PRESTO a parfois imposé une double tarification aux usagers et le tarif adulte régulier plutôt que le tarif réduit aux étudiants et aux aînés. En outre, les fonds n'ont pas toujours été versés à temps dans les cartes PRESTO des usagers, de sorte que celles-ci ont été refusées pour cause de fonds insuffisants.
- Metrolinx ne détermine pas si elle dispose de ressources suffisantes en personnel ou si elle devrait embaucher des employés à plein temps avant de recruter des sous-traitants à des taux beaucoup plus élevés. Nous avons constaté que les sous-traitants sont affectés à des postes de gestion clés et à des rôles décisionnels, y compris l'embauche et la surveillance d'autres sous-traitants. Elle dépend fortement des sous-traitants externes pour les activités et les services de TI et au cours des cinq dernières années, elle leur a versé environ 157 millions de dollars, ce qui correspond à environ le double et demie des salaires et avantages sociaux du personnel à plein temps.
- À l'exception du système de TI de PRESTO, Metrolinx n'a pas effectué d'analyses de sécurité régulières, comme des tests de pénétration, et elle n'examine pas toujours le code logiciel pour déceler les lacunes en matière de sécurité. Au cours des cinq dernières années, deux infractions importantes à la sécurité ont entraîné la divulgation des renseignements personnels des clients. Metrolinx n'applique pas de mesures de contrôle de sécurité, comme le chiffrement, pour protéger les renseignements personnels de ses usagers. En outre, Metrolinx ne dispose pas de stratégie de reprise après sinistre et n'a pas non plus mis à l'essai sa capacité de reprendre ses activités dans l'éventualité d'une catastrophe réelle, comme une grave attaque à la cybersécurité, des problèmes de logiciels découlant de changements imprévus ou des pannes d'électricité.
- Metrolinx n'a pas d'approche centralisée pour l'acquisition de sites Web et de systèmes de TI. Nous avons constaté que différents services ont procédé à leurs propres acquisitions de sites Web et systèmes de TI, ce qui s'est traduit par plusieurs systèmes de TI redondants.

## Conclusions

- Metrolinx ne dispose toujours de systèmes et de processus pour gérer ses activités de TI de façon efficace, efficiente ou économiquement sensée. Les services essentiels de transport en commun, dont PRESTO, ont subi les retombées négatives des problèmes liés aux systèmes de TI.
- Metrolinx dépend dans une trop grande mesure de la sous-traitance en ce qui touche l'exploitation courante des systèmes et services de TI. Metrolinx consacre davantage de fonds au personnel sous-traitant en TI qu'au personnel régulier à plein temps et, lorsqu'elle prend des décisions d'embauche, elle ne fait pas toujours en sorte que le personnel sous-traitant constitue un meilleur rapport qualité-prix.
- Les fonctions de cybersécurité de Metrolinx doivent être améliorées. À l'exception du système de TI de PRESTO, les renseignements personnels des employés et des clients de Metrolinx, ainsi que les renseignements de nature délicate sur l'organisation doivent être mieux sécurisés. Metrolinx n'a pas non plus de stratégie globale de TI, ce qui a entraîné la redondance des systèmes de TI et des sites Web.

Le rapport est accessible à l'adresse [www.auditor.on.ca](http://www.auditor.on.ca)