Chapitre 1
Section
1.05

Metrolinx

Suivi de la vérification de l'optimisation des ressources de 2020

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

APERÇU DE L'ÉTAT DES RECOMMANDATIONS

		État des mesures recommandées				
	Nombre de mesures recommandées	Pleinement mise en oeuvre	En voie de mise en oeuvre	Peu ou pas de progrès	Ne sera pas mise en oeuvre	Ne s'applique plus
Recommandation 1	1	1				
Recommandation 2	2	1	1			
Recommandation 3	4	3	1			
Recommandation 4	2	1	1			
Recommandation 5	1	1				
Recommandation 6	3	2	1			
Recommandation 7	4	4				
Recommandation 8	1	1				
Recommandation 9	1		1			
Recommandation 10	4	1	1	2		
Recommandation 11	2		2			
Recommandation 12	2	1	1			
Recommandation 13	2	1	1			
Recommandation 14	3	3				
Total	**32**	**20**	**10**	**2**	**0**	**0**
%	**100**	**63**	**31**	**6**	**0**	**0**

Conclusion globale

Le 31 août 2022, Metrolinx avait pleinement mis en oeuvre 63 % des mesures que nous avions recommandées dans notre Rapport annuel 2020. Par ailleurs, Metrolinx avait réalisé des progrès dans la mise en oeuvre de 31 % de nos recommandations.

Metrolinx a pleinement mis en oeuvre des recommandations comme l'analyse des causes fondamentales (ACF) des incidents de TI liés aux retards des trains par la création d'un tableau de bord mensuel pour détecter et résoudre les incidents de TI récurrents. Metrolinx avait également mis en oeuvre la recommandation consistant à établir un plan de cycle de vie des dispositifs pour remplacer les anciens dispositifs PRESTO désuets. Elle avait également amélioré le processus de gestion du changement des systèmes de TI afin de s'assurer que les changements sont autorisés, mis à l'essai et mis oeuvre sans provoquer d'erreurs. Pour surveiller

efficacement le rendement des fournisseurs, Metrolinx avait mis en oeuvre la recommandation de recevoir des rapports détaillés sur les incidents de la part du fournisseur. Elle avait reçu des rapports sur les incidents et participé à des réunions avec les fournisseurs sur une base mensuelle. Pour corriger les faiblesses en matière de cybersécurité, Metrolinx avait mis en oeuvre notre recommandation en établissant un plan annuel pour effectuer des tests périodiques de la sécurité, comme des essais de pénétration et des analyses des vulnérabilités, en se dotant d'un nouveau système de TI pour le balayage de sécurité. En outre, Metrolinx avait mis en oeuvre les recommandations relatives à la dépendance excessive à des soustraitants en TI. Pour ce faire, elle utilise maintenant un cadre documenté pour évaluer les capacités internes et effectuer des analyses coûts-avantages avant de recourir à des sous-traitants au lieu de mettre à contribution ses employés à temps plein. Metrolinx avait également donné suite à la recommandation voulant de mettre en place des capacités de journalisation des audits. Metrolinx a également pleinement mis en oeuvre la recommandation d'élaborer une stratégie de TI pour l'acquisition centralisée de systèmes et de services de TI. De plus, pour donner suite à la recommandation d'examiner les sites Web existants, Metrolinx a évalué la pertinence de tous les sites Web et a élaboré un plan de restructuration pour regrouper les sites Web existants et éliminer ceux jugés non pertinents.

Comme indiqué précédemment, Metrolinx avait également fait des progrès dans la mise en oeuvre de 31 % des recommandations. Celles-ci comprenaient la recommandation d'appliquer un Programme de garantie de service uniforme pour tous les services de Metrolinx. Cette recommandation est en voie de mise en oeuvre pour le service UP Express. Pour surveiller efficacement le rendement des fournisseurs en TI, Metrolinx avait réalisé des progrès en matière de responsabilisation de ses fournisseurs. Elle avait ajouté une clause contractuelle relative aux cibles de service manquées qui s'applique aux nouveaux fournisseurs retenus après décembre 2021. Metrolinx s'affairait toujours à apporter des modifications aux anciens contrats. Elle avait également mis en oeuvre un système de TI pour appliquer les politiques relatives aux mots de passe dans les systèmes de TI à ouverture de session unique, mais elle n'avait pas encore mis en oeuvre de système de TI pour gérer la base de données Oracle. Elle a également fait des progrès dans la recommandation de mettre en oeuvre une stratégie de reprise après sinistre; au moment du suivi, Metrolinx était en train d'opérationnaliser l'infrastructure requise pour effectuer des exercices d'essai de reprise après sinistre.

En outre, Metrolinx a fait des progrès dans la recommandation concernant le nombre excessif de sites Web existants. Elle est d'ailleurs en train de regrouper les 20 sites actuels en trois sites simplifiés et elle éliminera les sites jugés non pertinents d'ici avril 2023. Le service des TI avait également réalisé des progrès relativement à la recommandation d'établir une stratégie de TI et un processus d'approvisionnement centralisé avec une équipe spécialisée et un directeur. Dans le cadre de son processus d'approvisionnement, Metrolinx effectue des analyses qui lui permettent par exemple de dégager une liste des besoins opérationnels et d'évaluer les systèmes existants avant d'acheter de nouvelles technologies, afin de s'assurer qu'un système existant ne permettrait pas déjà de répondre au besoin opérationnel. Metrolinx a réalisé des progrès en ce qui concerne notre recommandation en matière de cybersécurité qui consiste à effectuer des examens de balayage des codes en mettant en place un système de TI. Nous avons remarqué que Metrolinx a intégré quatre systèmes de TI et qu'elle prévoit intégrer 26 autres systèmes pour effectuer des examens des codes.

Cependant, Metrolinx avait fait peu ou pas de progrès dans la mise en oeuvre de 6 % des recommandations. Peu de progrès ont été réalisés quant à la recommandation d'effectuer une évaluation pour classifier les données existantes conformément à sa politique de classification des données visant à chiffrer les données applicables. Metrolinx a également fait peu de progrès dans la recommandation de restreindre l'accès aux renseignements organisationnels de nature délicate.

L'état des mesures prises en réponse à chacune de nos recommandations est exposé ci-après.

Contexte

Les systèmes de technologie de l'information (TI) jouent un rôle essentiel dans la gestion courante des services de transport en commun à l'agence Metrolinx (Metrolinx). Au cours de l'exercice 2021-2022, Metrolinx a effectué au total 70 millions de trajets de passagers au moyen de huit lignes ferroviaires dans 68 gares de train du Réseau GO, du service ferroviaire Union-Pearson Express (UP Express) et ses quatre gares, et de 44 circuits d'autobus du Réseau GO. Les systèmes de TI servent à exécuter les fonctions essentielles du transport en commun, comme les signaux ferroviaires, les commutateurs et les bornes de tarification, ainsi que les systèmes d'information des usagers, qui présentent des mises à jour sur les horaires ainsi que les alertes et les perturbations des services. Metrolinx compte divers sites Web et systèmes de TI dont se servent, d'une part, les employés qui assurent la prestation des services de transport en commun et, d'autre part, les usagers qui se renseignent sur les tarifs et les horaires pour planifier les circuits à emprunter ou présentent des demandes de renseignements généraux.

De plus, Metrolinx supervise le fonctionnement de PRESTO, le système de tarification géré et mis en service par Accenture aux termes d'un contrat depuis 2006. Les services de tarification, dont le système PRESTO, sont également fortement tributaires des systèmes de TI.

Au cours de notre audit de 2020, nous avions constaté que Metrolinx avait commencé à donner suite à certaines de nos constatations. Elle en était à améliorer les processus de surveillance des sous-traitants, dont les examens de leur rendement. De plus, elle avait amorcé l'amélioration des processus de gestion des projets de TI, comme la documentation des approbations de projet, la surveillance des échéanciers et le suivi des coûts. Metrolinx était également en voie de recenser les principaux systèmes de TI pour analyser les retombées d'une éventuelle panne causée par une catastrophe sur les activités opérationnelles.

Nous avions notamment constaté ce qui suit :

- Des incidents fréquent de TI ont occasionné des retards dans les déplacements par train ou leur annulation, ce qui s'est traduit par la perte de revenus. Les services essentiels de transport en commun avaient fait l'objet à maintes reprises d'incidents de TI, comme des problèmes de connexion au réseau, des défaillances des systèmes et des anomalies dans les logiciels et le matériel, ce qui s'était traduit par des retards dans les déplacements par train ou leur annulation. De janvier 2015 à janvier 2020, les problèmes de logiciels et de matériel avaient causé plus de 4 500 retards et annulations de services ferroviaires du Réseau GO et du réseau UP Express. Au cours de cette période, les retards dans les déplacements par train ou leur annulation qu'on imputait aux incidents de TI avaient entraîné des désagréments pour les usagers et la perte de revenus d'environ 450 000 $ en raison des remboursements effectués dans le cadre du Programme de garantie de service.
- Metrolinx n'avait pas systématiquement mis à l'essai ses systèmes de TI pour déceler les risques liés à la cybersécurité. À l'exception du système de TI PRESTO, Metrolinx n'avait pas effectué d'analyses de sécurité périodiques, comme des essais de pénétration sur certains systèmes de TI essentiels et ses sites Web, afin de déceler les failles de sécurité. Nous avions constaté que Metrolinx avait fait l'objet de cyberattaques qui avaient porté atteinte à la protection des renseignements personnels de ses usagers.
- Des sous-traitants avaient été recrutés sans analyse obligatoire des autres options, et bon nombre d'entre eux avaient joué des rôles clés au chapitre de la prise de décisions. Avant de sous-traiter des ressources à tarif supérieur, Metrolinx n'avait effectué ni analyse des ressources dont elle disposait déjà ni examen pour déterminer si elle devait embaucher du personnel à plein temps. Elle dépendait fortement des sous-traitants externes pour les activités et les services de TI; au cours des cinq années précédentes, elle leur avait versé environ 157 millions de dollars, ce qui correspond à environ le double et demi des salaires et avantages sociaux du personnel

à plein temps. Au total, elle avait renouvelé à maintes reprises le contrat d'à peu près le tiers de ces sous-traitants pendant plus de deux ans, voire plus de cinq ans dans certains cas.

- Les sous-traitants assumaient des rôles de gestionnaires et de décideurs clés, notamment dans la supervision des budgets des projets ou l'embauche et la supervision de sous-traitants supplémentaires. De janvier 2015 à juillet 2020, environ 40 % (307 sur 764) des sous-traitants en TI embauchés pour appuyer au quotidien le fonctionnement et les services de TI avaient été supervisés par d'autres sous-traitants.
- Les anomalies dans les logiciels et le matériel des bornes de tarification PRESTO avaient posé plusieurs problèmes aux usagers. Ces problèmes étaient l'incapacité de distribuer les billets de transport en commun, les billets qui demeuraient coincés, l'affichage défectueux et la perte de connexion à Internet, qui mettaient les dispositifs hors service. De février 2016 à mai 2020, selon les données les plus récentes à ce sujet, plus de 45 000 incidents de ce genre avaient touché les bornes de tarification PRESTO utilisées pour le service UP Express et les trains et autobus du Réseau GO. Les deux dispositifs touchés par le plus grand nombre d'incidents de TI et qui avaient entraîné des retombées considérables sur les usagers étaient les distributeurs automatiques de billets et les processeurs de tarification des gares, les bornes vertes de paiement par CCP, qu'on trouve dans les gares.
- L'absence d'une stratégie et d'une gouvernance organisationnelles en matière de TI avait occasionné l'approvisionnement en systèmes de TI redondants et des dépassements de coûts dans les projets. Metrolinx n'avait pas centralisé ses acquisitions de sites Web et systèmes de TI. Nous avions constaté que différents services avaient procédé à leur propre approvisionnement en sites Web et en systèmes de TI, ce qui s'était traduit par plusieurs systèmes de TI redondants et la production en double de fonctions qui existaient déjà chez d'autres services de Metrolinx. De plus, les problèmes systémiques de gestion des projets de TI avaient occasionné des dépassements de coûts d'environ 152 millions de dollars, ce qui avait porté le coût total à 288 millions de dollars, un montant supérieur au double de celui de l'estimation initiale de 136 millions de dollars entre 2014-2015 et 2018-2019.
- Nous avions formulé 14 recommandations préconisant 32 mesures à prendre pour donner suite aux constatations de notre audit.

Metrolinx s'était engagé à prendre des mesures en réponse à nos recommandations.

État des mesures prises en réponse aux recommandations

Nous avons effectué des travaux d'assurance entre mars 2022 et août 2022. Nous avons obtenu de Metrolinx une déclaration écrite selon laquelle, au 18 novembre 2022, elle avait fourni à notre Bureau une mise à jour complète sur l'état des recommandations que nous avions formulées dans notre audit à l'origine, il y a deux ans.

Les problèmes de TI qui influent sur les services ferroviaires se traduisent par la perte de revenus

Recommandation 1

Pour recourir à l'analyse des causes fondamentales en vue de rehausser l'expérience vécue par les usagers et réduire les retards dans les déplacements par train ou les annulations, nous recommandons que Metrolinx

- *documente les incidents de TI qui occasionnent des retards ou des annulations, qu'elle enquête sur ces incidents, qu'elle en détermine les causes fondamentales et qu'elle prenne les mesures correctives nécessaires pour éviter que des incidents du même nature se produisent de nouveau.*

  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que les systèmes de TI et les composantes technologiques connexes des activités essentielles de transport en commun avaient fait l'objet de fréquents incidents, comme des problèmes de connectivité au réseau, des défaillances des systèmes et des anomalies au chapitre des logiciels et du matériel, ce qui s'est traduit par des retards dans les déplacements par train ou leur annulation. Bien que Metrolinx documente les renseignements de base sur les incidents de TI qui occasionnent des retards et des annulations, nous avons constaté que les renseignements clés, comme les causes fondamentales des incidents et les mesures prises pour les régler, n'étaient pas consignés. Or, de telles précisions étaient nécessaires à l'analyse et à l'évaluation pour éviter que des problèmes du même type se reproduisent fréquemment.

Lors de notre suivi, nous avons constaté que Metrolinx avait amélioré son processus actuel de gestion des problèmes en effectuant des analyses des causes fondamentales des incidents de TI récurrents et en créant des tableaux de bord du rendement mensuels qui permettent de détecter les incidents fréquents entraînant des retards dans les déplacements par train ou leur annulation. Cette analyse porte sur les répercussions sur les finances et les clients ainsi que sur les mesures à prendre pour mettre en place des correctifs permanents afin de s'assurer que les incidents de TI semblables qui ont une incidence sur le service du Réseau GO sont détectés et résolus.

Nous avons constaté que de décembre 2020 à octobre 2022, 44 analyses des causes fondamentales ont été effectuées pour les incidents de TI liés aux passages à niveau, à la signalisation ferroviaire, aux problèmes de matériel et aux bungalows le long des voies ferrées. De plus, nous avons examiné un échantillon de trois incidents liés à des capteurs aux passages à niveau défectueux, à une défaillance du matériel et à une panne d'électricité. Nous avons constaté que les trois incidents de TI étaient consignés et que des plans d'action avaient été élaborés pour mettre en place des correctifs permanents.

Recommandation 2

Pour favoriser l'achalandage dans le transport en commun et rehausser l'expérience vécue et la satisfaction éprouvée par les usagers de façon juste et transparente, nous recommandons que Metrolinx :

- *étudie la possibilité d'instaurer un processus systématique de remboursement des usagers de PRESTO pour les retards de service admissibles en vertu du Programme de garantie de service, de façon à ce qu'ils ne soient plus tenus de présenter eux-mêmes une demande de remboursement;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que Metrolinx avait mis en place un Programme de garantie de service aux termes duquel les tarifs des usagers sont remboursés si les trains du Réseau GO sont en retard de 15 minutes ou plus. Le programme exigeait que les usagers vérifient s'ils y avaient droit puis présentent une demande de remboursement sur le site Web du Réseau GO, où ils saisissaient la date du déplacement, la gare de départ, la gare d'arrivée, l'heure à laquelle le départ du train était prévu ainsi que le numéro de leur carte PRESTO. Même si Metrolinx disposait de la technologie et des données nécessaires pour rembourser automatiquement les clients admissibles au Programme de garantie de service au moyen de cartes PRESTO, les usagers de Metrolinx devaient quand même demander un remboursement.

Dans le cadre de notre suivi, nous avons examiné une analyse détaillée effectuée par Metrolinx pour déterminer la faisabilité d'instaurer un processus systématique de remboursement des usagers de PRESTO et nous avons remarqué que pour automatiser le processus, des bornes de paiement par CCG de PRESTO devaient être installés sur tous les trains, et pas seulement dans les gares du Réseau GO, pour déterminer avec exactitude le train utilisé par un client et traiter les remboursements. Comme les dispositifs de PRESTO ne sont installés que dans les gares du Réseau GO, Metrolinx ne peut pas savoir quel train un client a utilisé, parce que des trains peuvent être mis en service à de très courts intervalles durant les heures de pointe ou

parce que Metrolinx n'a pas de moyen de savoir si un usager se trouvait à bord d'un train durant la partie du trajet qui a été retardé, si celui-ci utilise une borne de paiement par CCG à l'embarquement, mais n'en utilise pas à son débarquement. Nous avons examiné l'analyse de faisabilité et avons constaté qu'un investissement de 73 millions de dollars serait nécessaire pour installer des bornes de paiement par CCG de PRESTO à bord des trains du Réseau GO et automatiser les remboursements. Compte tenu de l'importance de cet investissement, Metrolinx a décidé de maintenir le processus de libre-service actuel et d'élargir les tarifs admissibles pour inclure les billets en papier et électroniques.

- *évalue la faisabilité d'un programme de garantie de service uniforme pour les clients du Réseau GO et d'UP Express.*
  État : En voie de mise en oeuvre d'ici mars 2023.

Détails

Notre audit de 2020 avait révélé que le Programme de garantie de service de Metrolinx n'était pas exécuté de façon uniforme pour les usagers des trains du Réseau GO et du service ferroviaire UP Express; les critères ouvrant droit à un remboursement étaient différents. Nous avions constaté que ce programme offrait aux usagers des trains du Réseau GO un remboursement tarifaire complet si les déplacements en train étaient en retard de 15 minutes ou plus. Les clients d'UP Express sont admissibles à un remboursement de tarif si les trains sont retardés de plus de 45 minutes.

Lors de notre suivi, nous avons constaté que Metrolinx avait effectué un examen de la faisabilité de mettre en oeuvre un Programme de garantie de service uniforme et normalisé pour les déplacements en train et en autobus du Réseau GO et le service ferroviaire UP Express. Au moment de notre audit de 2020, il existait un programme de garantie de service pour les trains du Réseau GO. Metrolinx est aujourd'hui en train de déployer la même garantie de service qu'il offre aux usagers des trains du Réseau GO et aux usagers du service ferroviaire UP Express. La garantie de service aux usagers du service ferroviaire UP Express fonctionnera de la même façon que celle du Réseau GO, à savoir qu'elle s'appliquera elle aussi en cas de retard de 15 minutes. Nous avons examiné les résultats de l'analyse de faisabilité et constaté que Metrolinx avait tenu compte de l'incidence de l'offre d'une garantie de service UP Express sur les revenus et que celle-ci était estimée à environ 57 000 $ par année. Le programme de garantie de service d'UP Express devrait être mis en oeuvre d'ici mars 2023.

En outre, pour déterminer si une garantie de service peut être offerte pour les autobus du Réseau GO, Metrolinx a effectué une étude de cas portant sur 35 sociétés régionales de transport par autobus recensées partout dans le monde et a constaté qu'une seule de ces sociétés offrait une garantie de service pour les déplacements en autobus et que son mode d'application n'était pas automatisé. À la lumière de cette étude, Metrolinx a déterminé qu'il n'était pas raisonnable de mettre en oeuvre un programme de garantie de service pour les déplacements en autobus en raison de l'imprévisibilité de facteurs externes comme la circulation et les voies de détour. Il a aussi été constaté que la société de transport par autobus offrant la garantie de service avait observé une augmentation importante des demandes de remboursement frauduleuses. Compte tenu de ces facteurs, Metrolinx a décidé de ne pas élargir le programme de garantie aux déplacements en autobus, mais seulement au service ferroviaire UP Express.

Recommandation 3

Pour favoriser l'achalandage dans le transport en commun et rehausser l'expérience vécue et la satisfaction éprouvée par les usagers, nous recommandons que Metrolinx améliore la fiabilité des dispositifs et des cartes PRESTO par les moyens suivants :

- *passer en revue et analyser les causes fondamentales des incidents afin de déceler les anomalies dans les logiciels et les difficultés de connexion et de prendre des mesures correctives pour empêcher que ces incidents se produisent de nouveau;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions relevé un nombre important d'incidents de TI touchant les cartes et dispositifs PRESTO, les distributeurs automatiques de billets et les processeurs de tarification des gares. Les anomalies dans les logiciels et le matériel des bornes de tarification PRESTO posaient plusieurs problèmes aux usagers. De février 2016 à mai 2020, plus de 45 000 incidents de ce genre ont touché les bornes de tarification PRESTO utilisées pour UP Express et les trains et autobus du Réseau GO.

Lors de notre suivi, nous avons constaté que Metrolinx avait amélioré son système actuel de gestion des incidents qui sert à enregistrer et à résoudre les incidents de TI touchant les dispositifs PRESTO afin d'inclure également un module de gestion des problèmes. Ce système permet de regrouper les incidents similaires et récurrents, et d'ajouter une classification des causes fondamentales pour faciliter l'exécution d'une ACF. Lors de notre audit de 2020, nous avions constaté que Metrolinx avait effectué des analyses des causes fondamentales (ACF) pour les types d'incidents de TI de priorité 1 et de priorité 2 qui pourraient avoir une incidence importante sur les dispositifs PRESTO, mais pas pour ceux de priorité 3 ou 4.

Dans le cadre de notre suivi, nous avons constaté que des ACF sont effectuées pour tous les incidents prioritaires, y compris les incidents de priorité 3 et 4 qui touchent les dispositifs PRESTO.

Nous avons examiné une liste de tous les enregistrements d'incidents de novembre 2021 à novembre 2022 et constaté que 112 enregistrements avaient été créés pour détecter et résoudre les incidents de TI récurrents de priorité 3 et 4. Nous avons examiné un échantillon de cinq enregistrements d'incidents et constaté qu'une analyse des causes fondamentales a été effectuée pour tous les enregistrements, y compris une référence à des incidents similaires et des répercussions sur les clients et les opérations.

- *établir un plan de cycle de vie des dispositifs afin d'en assurer le remplacement en temps voulu, une fois ceux-ci devenus désuets et inopérants;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que les distributeurs automatiques de billets des gares du Réseau GO et d'UP Express servent à l'achat de billets en format papier, à l'achat de cartes PRESTO de même qu'au téléversement de fonds à partir d'espèces, de cartes de débit et de cartes de crédit. Nous avions constaté qu'au cours des cinq années précédentes, plus de 40 000 incidents de TI avaient mis ces distributeurs partiellement ou totalement hors service. Ces incidents étaient notamment attribuables à des anomalies dans les logiciels causées par des changements imprévus, des problèmes liés à l'interface entre les systèmes de TI et des défaillances du matériel empêchant les distributeurs d'émettre des billets à cause de problèmes mécaniques causés par le vieillissement des dispositifs. Parmi les autres incidents de TI, il y avait eu à titre d'exemple des défaillances de l'écran d'affichage des anciens dispositifs et un code de logiciel mal écrit qui a entraîné un mauvais fonctionnement des dispositifs et les a rendus inutilisables.

Lors de notre suivi, nous avons constaté qu'un plan détaillé de gestion des actifs de PRESTO avait été établi par Metrolinx en octobre 2021. Afin de l'établir, on avait effectué notamment un examen de tous les actifs de PRESTO et documenté l'âge des dispositifs, le cycle de vie de tous les dispositifs PRESTO, y compris les distributeurs automatiques de billets. Les actifs qui ont atteint leur fin de vie utile sont évalués de façon continue pour un remplacement éventuel. Nous avons constaté qu'au 1er septembre 2022, Metrolinx avait remplacé environ 2 700 dispositifs dans le cadre du plan de remplacement des actifs.

- *améliorer le processus actuel de gestion du changement afin de détecter les exceptions comme les changements imprévus ou les transactions effectuées en double et en retard;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que de nombreux incidents de TI avaient eu trait, à titre d'exemple, à des défaillances de l'écran d'affichage des anciens dispositifs et à un code de logiciel mal écrit qui

avait causé le mauvais fonctionnement des dispositifs et les avait rendus inutilisables. Après avoir analysé ces incidents, nous avions constaté que plus de la moitié étaient liés à l'expiration de la connexion ou à des anomalies dans les logiciels et le matériel. Bon nombre de ces problèmes avaient été causés par des changements imprévus.

Lors de notre suivi, nous avons constaté qu'en juillet 2021, Metrolinx a amélioré le processus de gestion du changement en élargissant la portée de son conseil consultatif sur les changements (CCC), qui examine maintenant les changements prévus et imprévus apportés aux systèmes de TI. Le CCC se réunit deux fois par semaine pour examiner tous les changements afin de s'assurer qu'ils sont mis à l'essai et approuvés par les intervenants appropriés (par exemple, les services des TI, de cybersécurité et des opérations) et qu'ils comprennent d'autres éléments nécessaires, comme un plan de mise en oeuvre, un plan de repli et l'incidence du changement. Selon ce nouveau processus, tous les changements sont approuvés par le CCC avant la mise en oeuvre finale. Nous avons examiné un échantillon de cinq billets de changement et constaté que les changements avaient été mis à l'essai et qu'ils étaient accompagnés des plans requis, qu'ils avaient été approuvés par les personnes requises et qu'ils avaient été mis en oeuvre sans provoquer d'erreur.

- *instaurer un processus pour calculer les pertes de revenus imputables aux incidents de TI et qui découlent de la mise hors service des dispositifs PRESTO, puis en tenir compte dans les futurs contrats conclus avec les fournisseurs de dispositifs de TI.*
  État : En voie de mise en oeuvre d'ici novembre 2023.

Détails

Lors de notre audit de 2020, nous avions constaté qu'entre février 2016 et mars 2020, plus de 3 500 incidents de TI concernant des bornes vertes de paiement par CCG avaient été signalés. Les problèmes liés à ces dispositifs dans une gare du Réseau GO fortement achalandée (comme la gare Union) risquent de se traduire par un nombre élevé d'usagers qui subissent des désagréments. Par exemple, le 25 février 2019, les dispositifs de la gare Union servant au paiement des tarifs étaient demeurés hors service et indisponibles pendant environ deux heures durant la mise à jour du système. Cette situation avait touché environ 35 000 usagers qui n'avaient pas pu acquitter les tarifs et avait entraîné une perte d'environ 315 000 $ en revenus de tarification. Nous avions également observé que Metrolinx n'avait fait ni l'analyse, ni l'évaluation des pertes de revenus imputables aux pannes des bornes vertes de paiement par CCP.

Lors de notre suivi, nous avons constaté que Metrolinx avait mis à jour ses contrats avec ses fournisseurs afin d'inclure une clause pour les tenir responsables de tout écart aux cibles de service. Il utilisera cette clause pour calculer la perte de revenus.

Les pertes de revenus ont été traitées par la création d'ententes d'ordre commercial associées à des ententes sur les niveaux de service (ENS) concernant la disponibilité du service et le temps de reprise du service après une panne. Nous avons examiné le contrat du fournisseur responsable de la gestion et du règlement des problèmes de TI avec les distributeurs automatiques de billets et nous avons constaté qu'un système de points calcule les réductions de service et la disponibilité et que Metrolinx est indemnisé pour tout manquement du fournisseur à rétablir le service. Le montant de l'indemnité est calculé conformément à des clauses standard incluses dans les contrats avec le fournisseur et le montant calculé est déduit de la facture de Metrolinx. Ce calcul des pertes de revenus a déjà été défini. Cependant, Metrolinx est en train de mettre à jour les contrats des fournisseurs pour inclure les calculs des pertes de revenus, le cas échéant. Au moment de notre suivi, les fournisseurs n'avaient pas manqué aux ENS définies de sorte qu'aucune de ces clauses n'avait dû être appliquée.

Recommandation 4

Pour effectuer un suivi efficace du rendement des fournisseurs de TI, nous recommandons que Metrolinx puisse, en ce qui concerne tous les fournisseurs :

- *recevoir des rapports détaillés sur les incidents à tous les niveaux de priorité, répartis par niveau de priorité, passer ces rapports en revue pour*

déterminer si les objectifs de rendement en matière de résolution sont atteints conformément à la période prescrite, puis prendre des mesures correctives au besoin;

État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que les contrats avec des tiers ne permettaient pas adéquatement à Metrolinx de surveiller le rendement des fournisseurs et de signaler les incidents aux échelons supérieurs. Nous avions constaté que les cibles de rendement étaient déclarées collectivement et que l'information sur le rendement des quatre niveaux de priorité (priorité 1, priorité 2, priorité 3 et priorité 4) était regroupée, plutôt que déclarée en fonction de chaque niveau de priorité comme le prévoit l'entente. Il est important de faire rapport de chaque niveau de priorité séparément, car chaque niveau de priorité nécessite une période de résolution différente.

Lors de notre suivi, nous avons constaté que Metrolinx avait mis en place des points de contact mensuels avec les fournisseurs pour obtenir des rapports sur les niveaux de service, faire le suivi du rendement et examiner tout incident avec quatre fournisseurs actuels du système PRESTO : Telus, Accenture, Sheidt & Bachmann et BAI Communications. Metrolinx reçoit maintenant des rapports mensuels des fournisseurs sur les incidents. Ceux-ci donnent un aperçu des incidents, de la disponibilité des services et du rendement par rapport aux ENS. Nous avons examiné un échantillon de procès-verbaux des réunions avec les quatre fournisseurs du système PRESTO ainsi qu'avec Flowbird, le fournisseur de Metrolinx identifié dans l'audit de 2020. Nous avons constaté que des réunions mensuelles sont tenues avec ces fournisseurs pour déterminer si les cibles de rendement relatives à la résolution sont atteintes dans les délais prescrits.

Nous avons confirmé que des représentants de Metrolinx et de PRESTO avaient participé aux réunions et consigné les incidents aux fins de discussion. En outre, Metrolinx peut demander les données brutes utilisées pour produire les rapports fournis par les fournisseurs s'il décide d'effectuer sa propre validation des résultats déclarés.

- *intégrer des dispositions aux contrats pour tenir les fournisseurs responsables et les inciter à atteindre les objectifs, et prévoir des sanctions si les objectifs sont ratés.*

  État : En voie de mise en oeuvre d'ici novembre 2023.

Détails

Lors de notre audit de 2020, nous avions constaté que Metrolinx n'analysait pas systématiquement l'information déclarée par Accenture pour déterminer si les cibles sont atteintes pour chacun des niveaux de priorité et qu'Accenture avait erronément classé des incidents de priorité 1 comme des incidents de priorité 2 dans 15 cas. De plus, nous avions constaté que le contrat conclu entre Metrolinx et Flowbird n'exigeait pas de rapports mensuels à propos des ententes sur les niveaux de service ni ne prévoyait de sanctions permettant à Metrolinx de tenir Flowbird responsable des cibles de résolution des incidents non respectées à chaque niveau de priorité.

Lors de notre suivi, nous avons constaté que tous les nouveaux contrats conclus depuis décembre 2021 comprennent un ensemble normalisé de clauses qui rendent obligatoire la production de rapports sur le rendement des fournisseurs et la tenue de réunions. Nous avons examiné un extrait de ces clauses contractuelles en vigueur depuis décembre 2021 et constaté qu'elles prévoient systématiquement des déductions de frais sur les factures des fournisseurs en fonction de la disponibilité du service ou du temps requis pour rétablir le service après un incident.

Bien que ces clauses aient été incluses dans le contrat avec Flowbird, nous avons constaté que dans le cas des contrats existants et à caractère évolutif, comme celui conclu avec Accenture avant décembre 2021, on avait retenu les services d'un cabinet d'avocats tiers pour élaborer des clauses améliorées qui seront incluses dans les nouveaux contrats utilisés dans le cadre du processus d'approvisionnement. Ce processus était en cours au moment de notre suivi.

Dépendance et recours excessifs aux sous-traitants en TI

Recommandation 5

Pour que la gestion des membres du personnel contractuel soit efficace, nous recommandons que Metrolinx observe la Directive en matière d'approvisionnement de la fonction publique de l'Ontario et exige que les principaux rôles et responsabilités soient confiés à ses gestionnaires de la TI qualifiés et en poste à plein temps.

État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que les sous-traitants jouaient des rôles de gestion clés à Metrolinx. Environ 80 % (246) des 307 sous-traitants en TI relevaient de trois sous-traitants qui occupaient des postes de gestion. Ces trois sous-traitants prenaient des décisions concernant la budgétisation des projets et le recrutement de sous-traitants parmi les fournisseurs de services de dotation, ce qui outrepassait la Directive en matière d'approvisionnement de la fonction publique de l'Ontario.

Lors de notre suivi, nous avons constaté que Metrolinx avait réduit son nombre total de sous-traitants en TI de 243 en mars 2021 à seulement 57 en mars 2022, tout en faisant passer son effectif à temps plein de 148 à 262. Nous avons examiné le titre du poste de ces 57 sous-traitants en TI et constaté qu'aucun d'entre eux ne jouait de rôles de gestion clés à Metrolinx.

Recommandation 6

Pour doter en ressources de façon efficace et économique les projets de TI et observer la Directive en matière d'approvisionnement de la fonction publique de l'Ontario, nous recommandons que Metrolinx :

- *analyse la capacité interne des ressources en TI avant de décider de retenir les services de sous-traitants;*

  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté qu'aux termes de la Directive en matière d'approvisionnement de la FPO, il faut d'abord envisager le recours aux ressources internes avant de décider de retenir les services d'experts-conseils externes. Metrolinx avait versé environ 157 millions de dollars aux sous-traitants en TI, ce qui correspond à environ le double et demi du montant consenti en salaires et en avantages sociaux aux membres de son personnel, alors que le total des coûts des employés à plein temps en TI se chiffrait à environ 65 millions de dollars. D'après notre examen d'un échantillon de 25 dossiers de recrutement de sous-traitants, nous avons constaté que Metrolinx n'avait consigné aucun examen de la capacité interne, contrairement à sa propre politique et à la directive de la FPO qui exige clairement un examen de la capacité interne et une analyse coûts-avantages de l'embauche d'un employé à temps plein avant de retenir les services d'un sous-traitant.

Lors de notre suivi, nous avons constaté que Metrolinx avait mis en oeuvre un processus documenté pour examiner la pertinence d'embaucher du personnel à temps plein avant de choisir de retenir les services d'un sous-traitant. Chaque fois qu'une demande de ressources lui est présentée, Metrolinx effectue une évaluation pour déterminer le personnel interne peut y répondre. Si tel est le cas, la demande est traitée. Dans le cas contraire, une autre évaluation est effectuée pour déterminer si le recours à un sous-traitant est nécessaire ou si un employé à temps plein peut être embauché. Ce processus doit être approuvé par un vice-président avant qu'un sous-traitant puisse être recruté. Il fait partie du cadre global créé par Metrolinx pour revoir le processus de gestion des ressources concernant les sous-traitants et le personnel à temps plein. Sur un total de 57 sous-traitants en TI existants, nous avons sélectionné un échantillon de cinq sous-traitants et examiné l'évaluation des capacités internes. Nous avons observé que pour les cinq postes de sous-traitants en TI, Metrolinx avait effectué une évaluation de la capacité interne avant de recruter le sous-traitant et que la demande d'embauche du sous-traitant avait été approuvée par le vice-président.

- *effectue des analyses coûts-avantages pour évaluer l'économie et l'à-propos quant à la rétention des services de sous-traitants plutôt que l'embauche*

d'employés à plein temps, surtout lorsque les ressources seront vraisemblablement requises à long terme;

État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, après avoir examiné un échantillon de 25 dossiers de recrutement de sous-traitants, nous avions constaté que Metrolinx n'avait pas documenté d'examen de la capacité interne ni effectué d'analyse coûts-avantages quant à l'embauche de sous-traitants plutôt que d'employés à plein temps. Cette façon de faire outrepasse la propre politique de Metrolinx en la matière ainsi que la Directive en matière d'approvisionnement de la FPO, laquelle exige clairement d'effectuer une analyse coûts-avantages pour l'embauche d'un employé à plein temps avant l'embauche d'un sous-traitant.

Lors de notre suivi, nous avons constaté que l'analyse coûts-avantages faisait partie du cadre mis à jour qui privilégie le personnel à temps plein plutôt que le recours à des sous-traitants. Une fois qu'il est déterminé qu'un employé interne à temps plein ne peut pas être mis à contribution pour répondre à une demande de ressources, une évaluation est effectuée pour déterminer si un sous-traitant est nécessaire ou si la demande vise un besoin à long terme et qu'un employé à temps plein peut être embauché. Sur un total de 57 sous-traitants en TI existants, nous avons sélectionné un échantillon de 5 sous-traitants et examiné leurs dossiers de recrutement pour déterminer si Metrolinx avait effectué une analyse coûts-avantages. Nous avons constaté qu'une évaluation avait été effectuée dans le cas des cinq sous-traitants afin de garantir la valeur économique et la pertinence de retenir les services de sous-traitants plutôt que d'embaucher des employés à temps plein.

- *mène des entrevues, documente celles-ci et conserve les notes s'y rapportant, dont les approbations requises avant de retenir les services de sous-traitants.*

  État : En voie de mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté qu'aucune documentation ne permettait de justifier le recours à de nouvelles ressources, ni d'attester l'obtention en bonne et due forme par les gestionnaires responsables de l'embauche d'approbations pour retenir les services de sous-traitants. Dans 23 des 25 dossiers de recrutement de sous-traitants que nous avons passés en revue, Metrolinx ne disposait d'aucune documentation relative aux candidats interviewés concernant les rôles des sous-traitants, ni des notes d'entrevue, ni des noms des employés qui ont pris part aux travaux du comité d'entrevue.

Lors de notre suivi, nous avons constaté que Metrolinx avait établi un processus centralisé identique à celui mis en oeuvre aux fins du recrutement du personnel à temps plein, dans le cadre duquel une note calculée est attribuée à tous les candidats pour un rôle en fonction des réponses documentées aux questions d'entrevue. Nous avons sélectionné neuf dossiers de recrutement des sous-traitants en TI embauchés après notre audit de 2020 afin d'évaluer si les notes d'entrevue étaient documentées et si les noms des employés qui ont pris part aux travaux du comité d'entrevue étaient indiqués. Nous avons constaté que dans le cas de cinq sous-traitants en TI, Metrolinx n'avait pas consigné ni conservé les notes d'entrevue. Nous avons également remarqué que deux de ces cinq sous-traitants en TI avaient été embauchés directement, en contournant le processus d'entrevue, sans justification formelle. À la suite de notre examen, Metrolinx s'est engagé à mettre pleinement en oeuvre cette recommandation en documentant et en conservant les notes d'entrevue dans toutes les embauches futures de sous-traitants.

Recommandation 7

Pour qu'elle gère ses ressources en TI de façon pertinente et performante, nous recommandons que Metrolinx :

- *respecte la Directive en matière d'approvisionnement de la fonction publique de l'Ontario et documente le motif du renouvellement ou de la prolongation des contrats;*

  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que Metrolinx n'avait pas fourni de justification appropriée ni n'avait évalué le rendement des fournisseurs avant de renouveler ou de prolonger les contrats des sous-traitants. D'après l'échantillon de 25 sous-traitants en TI examiné par le Bureau, 20 d'entre eux (ou 80 %) avaient obtenu de leur gestionnaire la prolongation de leur contrat.

Lors de notre suivi, nous avons constaté que chaque renouvellement de contrat de sous-traitance doit maintenant être accompagné d'une justification documentée et d'une approbation du vice-président, laquelle est stockée dans un système de TI. Nous avons examiné un échantillon de cinq documents de renouvellement de contrat et constaté que les cinq sous-traitants avaient reçu une justification adéquate et documentée, approuvée par un vice-président, avant la prolongation de leur contrat.

- *confirme, au moyen d'évaluations du rendement, que le sous-traitant présente un rendement satisfaisant et obtienne les approbations nécessaires avant le renouvellement ou la prolongation du contrat;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté qu'aucune des 20 prolongations de contrat examinées n'était fondée sur un motif économique ou sur une évaluation du rendement menée par leur gestionnaire pour attester le caractère satisfaisant de leur travail.

Lors de notre suivi, nous avons constaté qu'en mars 2021, le groupement de l'ITI effectuait une évaluation du rendement avant chaque renouvellement de contrat et départ de sous-traitant. Nous avons examiné cinq échantillons des examens du rendement et constaté que l'évaluation note la satisfaction des exigences techniques par le sous-traitant et son professionnalisme, et documente la volonté du gestionnaire de réembaucher le sous-traitant et de prolonger son contrat. Nous avons également observé que les cinq prolongations de contrat avaient été dûment approuvées par un vice-président par courriel avant la prolongation du contrat.

- *analyse le motif des bonifications aux taux horaires des sous-traitants afin que les taux révisés soient économiques;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que les sous-traitants recevaient régulièrement des bonifications de taux sans que les motifs les justifiant soient documentés. D'après l'échantillon de 25 dossiers de recrutement de sous-traitants que nous avions examinés dans les 5 années précédentes (au moment de notre audit), nous avions constaté que Metrolinx avait consenti des taux horaires bonifiés à 12 (48 %) des 25 sous-traitants. Or, ces bonifications ne reposaient sur aucun motif clairement indiqué, comme l'avancement à un poste de niveau supérieur ou l'attribution de responsabilités accrues. Les bonifications des taux horaires oscillaient entre 4 % et 12 %.

Lors de notre suivi, nous avons constaté que Metrolinx avait mis en oeuvre un nouveau processus de gestion des fournisseurs pour s'assurer que tout sous-traitant qui demande une bonification des taux voit sa demande examinée afin de déterminer si elle est justifiée, dans lequel cas elle est approuvée par le vice-président compétent. Dans le cadre du processus de gestion des fournisseurs, Metrolinx examine le mandat du sous-traitant et le moment où la dernière bonification de taux a été accordée et effectue une comparaison avec les autres sous-traitants jouant le même rôle dans le cadre du même contrat. La bonification des taux pour chaque rôle ne peut entraîner le dépassement du taux maximal établi. La bonification des taux doit également être approuvée par le vice-président et le dirigeant principal de l'information concerné avant que le contrat puisse être modifié. Nous avons examiné les dossiers des trois sous-traitants dont les taux avaient été bonifiés et nous avons constaté que ces trois bonifications avaient été dûment approuvées par un vice-président compétent et par le dirigeant principal de l'information, et que les motifs les justifiant avaient été documentés. Nous avons également examiné trois demandes de bonification de taux rejetées et constaté qu'une demande de bonification du taux horaire d'un

sous-traitant au-delà du maximum prévu pour ce rôle avait été rejetée, et que le motif documenté était le dépassement du taux maximum. Nous avons également relevé deux autres cas où des sous-traitants qui avaient demandé qu'on leur attribue un rôle assorti d'un taux plus élevé avaient aussi vu leur demande refusée, car ils n'avaient pas été en mesure de fournir explication détaillée justifiant qu'on leur attribue le rôle demandé assorti d'un taux horaire plus élevé.

- *effectue une analyse qualitative et quantitative complète de sa stratégie d'impartition et obtienne l'approbation du conseil d'administration et du ministère avant d'apporter des changements stratégiques considérables, comme l'impartition du service de TI.*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté qu'en avril 2020, Metrolinx avait pour stratégie d'accroître l'embauche d'employés à plein temps plutôt que de retenir les services de sous-traitants afin d'amoindrir la dépendance excessive à l'égard de ces derniers, de diminuer les coûts et de favoriser le maintien du savoir au sein de l'agence. Le pourcentage des sous-traitants par rapport aux employés à plein temps s'est accru et il est passé de 40 % à 63 % de 2015-2016 à 2019-2020. Cette stratégie avait été présentée au conseil d'administration, au chef de la direction et à l'équipe des cadres supérieurs de Metrolinx, après quoi on avait autorisé le service à embaucher à plein temps environ 60 employés en TI. N'empêche, en août 2020, nous avions constaté que Metrolinx avait envisagé de retenir les services d'une firme de recherche pour élaborer des options d'impartition de certaines activités au sein du service de TI afin de transférer les risques liés à la technologie à un tiers fournisseur.

Lors de notre suivi, nous avons constaté que Metrolinx n'avait imparti aucune de ses fonctions de technologie de l'information comme celles liées relevant des divisions du bureau de gestion des projets, de l'infrastructure de TI, du développement et à la livraison de solutions de TI, de l'architecture de la TI et de la sécurité de l'information. Metrolinx a plutôt embauché un nouveau dirigeant principal de l'information et quatre vice-présidents pour gérer les quatre divisions de la technologie susmentionnées. De plus, Metrolinx a indiqué s'il devait prendre des décisions importantes, comme l'impartition de l'ensemble des fonctions assumées par la division de la technologie de l'information, il demanderait l'approbation du ministère des Transports et de son conseil d'administration.

Lacunes au titre de la sécurité des systèmes de TI de Metrolinx

Recommandation 8

Pour réduire la vulnérabilité de Metrolinx aux cyberattaques et à la divulgation accidentelle de renseignements, nous recommandons que l'entreprise atténue ses risques et protège de façon efficace ses systèmes de TI en effectuant des tests de sécurité périodiques, comme des essais de pénétration, sur ses sites Web et systèmes de TI essentiels, conformément aux normes sectorielles.
État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que Metrolinx n'avait pas effectué de mise à l'essai régulière de la sécurité des systèmes de TI pour cerner les faiblesses et prévenir les atteintes à l'intégrité. À l'exception du système de TI PRESTO, nous avions constaté que, depuis des années, Metrolinx n'effectuait pas régulièrement d'essais de pénétration des sites Web et systèmes de TI essentiels. Nous avions donc conclu que les systèmes de la TI étaient vulnérables aux attaques; de fait, deux atteintes graves à la sécurité avaient eu lieu dans les cinq années précédentes.

Lors de notre suivi, nous avons constaté que Metrolinx avait mis en place un nouveau système de TI pour effectuer des mises à l'essai régulières, y compris des analyses des vulnérabilités portant sur les nouvelles versions de produits et les changements majeurs. En outre, Metrolinx a élaboré un calendrier d'exécution des analyses des vulnérabilités et des essais de pénétration. Nous avons examiné le calendrier des essais de sécurité des deux dernières années et tous les essais de pénétration effectués depuis notre audit de 2020.

Nous avons constaté que Metrolinx effectuait régulièrement des essais de pénétration de son réseau de TI et de chacun de ses systèmes de TI. De plus, nous avons remarqué que les essais de pénétration du réseau des TI avaient été répétés pour s'assurer que les faiblesses cernées dans les essais précédents avaient été corrigées. Tous les systèmes de TI mentionnés dans l'audit précédent ont été inclus dans ces essais de pénétration et les vulnérabilités ont été cernées et corrigées.

Recommandation 9

Pour que Metrolinx puisse protéger de façon efficace ses systèmes de TI contre le risque de cyberattaque causé par des failles de sécurité, nous recommandons qu'elle réexamine à intervalles réguliers les codes logiciels essentiels et fondamentaux des réseaux de transport en commun, conformément aux pratiques exemplaires du secteur.

État : En voie de mise en oeuvre d'ici mars 2023.

Détails

Lors de notre audit de 2020, nous avions constaté que Metrolinx n'avait pas examiné le code logiciel pour cerner les lacunes en matière de sécurité. Nous avions constaté que le code logiciel des 12 systèmes de TI échantillonnés pour en déceler les failles de sécurité n'avait pas été réexaminé. Selon les pratiques exemplaires du secteur, il convient que les organisations réexaminent les codes logiciels chaque fois que des changements sont apportés aux systèmes de TI essentiels en vue de cerner les failles de sécurité.

Lors de notre suivi, nous avons constaté que Metrolinx avait mis en place un nouveau système de TI qu'il utilise pour effectuer des examens des codes logiciels de ses systèmes de TI. Tous les nouveaux projets sont soumis au processus d'examen du code pour repérer les erreurs. Toutes les erreurs repérées doivent être corrigées ou soumises à un processus formel en vue d'une exception avant la mise en service. Nous avons examiné un échantillon de codes et nous avons confirmé que les erreurs étaient signalées à des fins de correction. Au moment du suivi, nous avons constaté que quatre systèmes de TI avaient été intégrés au système d'examen des codes et que des examens des codes avaient été menés. Metrolinx procède actuellement à l'intégration de 26 autres systèmes de TI au système d'examen des codes. Metrolinx indique que tous les nouveaux systèmes de TI mis en oeuvre seront intégrés au système de TI d'examen des codes.

Recommandation 10

Pour protéger efficacement les renseignements et se conformer aux exigences de la Loi sur l'accès à l'information et la protection de la vie privée, nous recommandons que Metrolinx :

- *protège tous les renseignements personnels par le classement, le masquage et le chiffrement des données selon les pratiques exemplaires du secteur;*
  État : Peu ou pas de progrès.

Détails

Lors de notre audit de 2020, nous avions constaté que les renseignements personnels des clients de Metrolinx n'étaient pas tous protégés de manière adéquate. À l'exception de PRESTO, nous avions constaté dans notre examen que Metrolinx n'identifie, ne classe et ne protège pas de façon cohérente les renseignements personnels des usagers et des employés. Or, puisque ces renseignements sont visés par la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) de l'Ontario, elle est tenue de stocker et de transférer des renseignements personnels de façon sécuritaire, et de créer un inventaire à jour annuel des renseignements personnels de ses usagers.

Lors de notre suivi, nous avons constaté que Metrolinx n'avait pas effectué d'évaluation conformément à sa politique de classification des données pour repérer les données de nature hautement délicate et assurer une protection adéquate comme le chiffrement. Metrolinx a mis en oeuvre un système de TI utilisé pour analyser et repérer les renseignements personnels identificatoires (RPI). Nous avons constaté que Metrolinx était en train de recenser les systèmes de TI qui contiennent des renseignements de nature hautement délicate, conformément à sa politique sur la sécurité de l'information. L'évaluation devrait être terminée d'ici le 1er mai 2023.

- *limite l'accès à ses renseignements organisationnels de nature délicate, conformément aux normes et aux pratiques exemplaires du secteur;*
  État : Peu ou pas de progrès.

Détails

Lors de notre audit de 2020, nous avions constaté que Metrolinx compte actuellement sept administrateurs de bases de données de la TI qui ont pleinement accès à deux bases de données pour y lire et modifier les renseignements personnels confidentiels des usagers et employés de Metrolinx. De plus, trois des sept administrateurs de bases de données de TI étaient des soustraitants et non des employés à plein temps de Metrolinx. Nous avions également constaté que quatre administrateurs de la base de données Oracle s'échangeaient les noms d'utilisateur et mots de passe des administrateurs, ce qui réduisait la probabilité que Metrolinx puisse déterminer à qui il incombait de rendre compte dans l'éventualité d'une erreur ou d'une atteinte à la confidentialité.

Lors de notre suivi, nous avons constaté que Metrolinx n'avait pas limité ou éliminé l'accès excessif à ses bases de données qui stockent des renseignements confidentiels. De plus, nous avons constaté que les mots de passe étaient encore échangés entre les quatre administrateurs identifiés dans notre audit. En revanche, Metrolinx a lancé un projet de gestion des accès privilégiés afin de mettre en oeuvre un système de TI permettant de stocker et d'échanger en toute sécurité les identifiants des administrateurs. Nous avons examiné la portée du projet et constaté que la feuille de route du projet sera créée d'ici novembre 2022. De plus, nous avons examiné quatre procès-verbaux de réunions bimensuelles établis par Metrolinx et constaté qu'il examine tous les changements ou ajouts apportés à tous les groupes d'administrateurs.

- *passe en revue les paramètres des mots de passe relatifs aux systèmes essentiels de la TI pour ensuite appliquer sa politique sur les mots de passe afin de réduire le risque d'accès non autorisé;*
  État : En voie de mise en oeuvre d'ici mars 2023.

Détails

Lors de notre audit de 2020, nous avions constaté que quatre administrateurs de la base de données Oracle s'échangeaient les noms d'utilisateur et mots de passe des administrateurs, ce qui réduisait la probabilité que Metrolinx puisse déterminer à qui il incombe de rendre compte dans l'éventualité d'une erreur ou d'une atteinte à la confidentialité.

Lors de notre suivi, nous avons constaté que Metrolinx était en train de mettre en oeuvre un nouveau système de TI qui appliquera les politiques relatives aux mots de passe afin de réduire le risque d'accès non autorisé. Au moment de notre suivi, des politiques relatives aux mots de passe avaient été appliquées à tous les systèmes de TI qui utilisent l'authentification Microsoft Windows. Cependant, Metrolinx est encore en train de mettre en oeuvre le système de TI qui permettra d'appliquer les politiques relatives aux mots de passe dans les systèmes de TI qui exploitent leur propre processus d'authentification. Le 1er septembre 2022, 22 systèmes de TI avaient été intégrés au système de TI appliquant les politiques relatives aux mots de passe. Metrolinx procède également à la migration de son système de TI Oracle vers le système de TI appliquant les politiques relatives aux mots de passe qui permettra l'authentification multifactorielle pour accéder à Oracle.

- *instaure des capacités de journalisation des audits et des alertes en ce qui touche les événements nécessaires pour garantir l'obligation de rendre compte et la protection des renseignements.*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que Metrolinx ne consignait pas les activités nécessaires dans l'éventualité où une table de la base de données serait modifiée ou supprimée. Les journaux détaillés des bases de données et les activités de suivi exécutées par les administrateurs des bases de données permettent aux organisations d'établir l'obligation de rendre compte, de repérer les modifications non autorisées aux données et de déceler les activités frauduleuses.

Lors de notre suivi, nous avons constaté que Metrolinx avait installé un système de TI qui sert à surveiller les menaces à la sécurité des TI sur son réseau. Nous avons examiné un rapport portant des menaces détectées en janvier 2022, comme des cas d'hameçonnage et de virus informatiques. Il documentait la gravité de l'incident et l'état de la résolution. De plus, nous avons remarqué que des capacités de journalisation d'audit avaient été mises en oeuvre pour la base de données Oracle en août 2021.

Absence de stratégie de reprise après sinistre

Recommandation 11

Pour améliorer la lutte contre les risques qui menacent les systèmes de technologie de l'information dont le rôle est essentiel à la prestation des services de transport en commun, nous recommandons que Metrolinx :

- *détermine une stratégie de reprise après sinistre, pour ensuite planifier et exécuter à intervalles réguliers des exercices de reprise après sinistre afin de minimiser le plus possible les perturbations causées par des incidents de TI;*
  État : En voie de mise en oeuvre d'ici mars 2023.

Détails

Lors de l'audit de 2020, nous avions constaté que Metrolinx n'avait pas de stratégie de reprise après sinistre (RS) ni n'exécutait des exercices de reprise après sinistre à des intervalles réguliers. Le Bureau avait constaté que l'agence Metrolinx n'avait pas établi de stratégie organisationnelle de reprise après sinistre pour garantir la continuité des activités commerciales.

Au moment de notre suivi, nous avons constaté que Metrolinx était en train d'élaborer une stratégie de RS et de mettre en place l'infrastructure requise pour que la stratégie soit opérationnelle. Les exercices de RS n'étaient pas encore effectués, mais Metrolinx avait déjà évalué ses systèmes de TI pour déterminer les 54 systèmes les plus vulnérables et avait établi un plan pour élaborer un exercice de reprise après sinistre pour les 54 systèmes de TI vulnérables. Nous avons examiné un calendrier du projet de RS et constaté que la capacité de RS devrait être entièrement opérationnelle pour 20 des 54 systèmes de TI essentiels désignés par Metrolinx d'ici octobre 2022 et que les autres systèmes de TI devraient suivre.

- *procède à une analyse coûts-avantages pour déterminer un lieu fonctionnel de reprise après sinistre aux fins de la continuité du transport en commun.*
  État : En voie de mise en oeuvre d'ici mars 2023.

Détails

Lors de notre audit, nous avions constaté que le Centre de données de Kingston était le site de RS de Metrolinx. Toutefois, le Centre de données de Kingston n'est pas doté des serveurs, logiciels et données nécessaires pour fonctionner comme autre emplacement dans l'éventualité d'une catastrophe. Puisqu'une catastrophe au Centre de données de Guelph pourrait causer des retards importants aux services de transport en commun, il convient d'établir des sauvegardes et des redondances pour minimiser le plus possible les pannes de service.

Lors de notre suivi, nous avons constaté que Metrolinx avait effectué une analyse coûts-avantages et choisi un centre de données privé à Barrie, en Ontario, qui servirait de site de RS pour tous les systèmes applicables. Nous avons examiné le contrat entre Metrolinx et le fournisseur propriétaire du centre de données de Barrie qui a été signé le 1er octobre 2021. Au moment du suivi, l'infrastructure requise pour que le site devienne opérationnel était en cours d'installation. Nous avons également remarqué qu'aucun exercice complet de RS n'avait encore été effectué.

L'absence de stratégie de TI occasionne un dédoublement des coûts et des ressources, et des dépassements de coûts évitables dans les projets de TI

Recommandation 12

Pour réduire le dédoublement des coûts et des initiatives en double et améliorer la surveillance du fonctionnement de la TI, nous recommandons que Metrolinx :

- *établisse une stratégie globale de TI assortie d'un processus d'approvisionnement centralisé pour les systèmes et services de TI;*
  État : Pleinement mise en oeuvre.

Détails

Lors de l'audit de 2020, nous avions constaté que les projets de TI ne disposaient pas d'un processus d'approvisionnement centralisé pour éviter le dédoublement des coûts et les dépassements de coûts évitables. À Metrolinx, l'acquisition des systèmes de TI est décentralisée, sans stratégie globale ni surveillance efficace. Selon la Directive en matière d'approvisionnement de la fonction publique de l'Ontario, il y a lieu que les organisations valident l'existence des mêmes biens et services à l'interne avant d'amorcer un nouveau processus d'approvisionnement.

Lors de notre suivi, nous avons constaté qu'en août 2021, un nouveau directeur de l'approvisionnement en services d'ITI a été embauché pour diriger une équipe spécialisée en approvisionnement. Metrolinx a établi une stratégie qui stipule que tout approvisionnement est facilité par l'équipe d'approvisionnement en services d'ITI spécialisée. Il existe un processus qui prévoit de s'adresser d'abord aux fournisseurs attitrés existants de Metrolinx, puis justifier et obtenir l'approbation de l'équipe d'approvisionnement de recourir à un autre fournisseur externe. Pour tous les nouveaux systèmes de TI que Metrolinx désire mettre en oeuvre, le projet doit faire l'objet d'un examen complet de l'architecture avant de demander du financement, afin de s'assurer que la technologie existante est utilisée dans la mesure du possible. Nous avons examiné un système de TI récemment acquis, Microsoft Customer Insights, qui fournit des données analytiques à partir du système de TI existant de Metrolinx. Nous avons constaté que les documents d'approvisionnement faisaient état des exigences opérationnelles et qu'elles avaient été comparées à celles de deux autres systèmes de TI existants de Metrolinx dans tous les secteurs afin de vérifier que les systèmes existants ne permettraient pas de répondre pas adéquatement ou de façon rentable à ces exigences. En ce qui concerne les systèmes de TI échantillonnés et examinés dans le cadre de l'audit de 2020, nous avons constaté que Metrolinx avait effectué une évaluation et qu'il était en train de remplacer des systèmes de TI en double.

- *surveille et analyse le besoin en systèmes ou dispositifs actuels de TI installés dans tous ses services, pour ensuite déterminer un processus servant à déterminer s'il existe déjà un système de TI à l'interne avant d'en acquérir de nouveaux.*
  État : En voie de mise en oeuvre d'ici octobre 2023.

Détails

Lors de notre audit, nous avions constaté que certains secteurs de service avaient acquis d'autres systèmes et services de TI tandis que d'autres disposaient déjà des mêmes systèmes ou fonctions que ceux recherchés. La décentralisation dans la gouvernance de la TI à Metrolinx s'était traduite par un manque de connaissances centralisées sur les systèmes de TI utilisés dans les divers secteurs de service de l'organisation.

Lors de notre suivi, nous avons constaté qu'en février 2022, les secteurs de l'approvisionnement, de l'ITI et du bureau commercial de Metrolinx avaient conjointement mis en place un forum mensuel de gestion des relations qui appuie la stratégie, la planification, l'établissement de la priorité et la surveillance des transactions d'approvisionnement en TI. Une réunion informelle stratégique est également tenue chaque semaine avec des intervenants, y compris le dirigeant principal de l'information, le vice-président des TI, le directeur de l'approvisionnement, le vice-président commercial et le directeur commercial. Nous avons examiné une évaluation effectuée par Metrolinx pour repérer les systèmes de TI en double et constaté que 32 systèmes avaient été recensés et qu'une stratégie était en place pour tirer parti de la technologie existante, lorsque cela est possible.

Recommandation 13

Pour que Metrolinx économise et réalise des gains d'efficience, nous recommandons qu'elle :

- *fasse l'examen des sites Web actuels;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que Metrolinx disposait en tout de 20 sites Web différents offrant des fonctions qui se chevauchent, des renseignements semblables et générant des coûts de développement inutiles. Metrolinx disposait en tout de huit sites Web destinés aux usagers dotés de diverses fonctions comme l'achat de billets, la planification des trajets, les horaires et les mises à jour des services. Au total, elle avait assumé des coûts d'immobilisations d'environ 44 millions de dollars pour le développement de ces sites Web et, chaque année, elle versait environ 14 millions de dollars à divers fournisseurs qui en assuraient la maintenance et le fonctionnement.

Lors de notre suivi, nous avons noté que Metrolinx a élaboré un plan de développement visant à regrouper les 20 sites Web en double en trois sites uniques. L'élaboration des sites Web avait commencé au moment de notre suivi et un calendrier de mise en oeuvre était disponible. Le premier site Web consolidé sera mis en ligne en septembre 2022 et tous les autres sites Web en double seront regroupés et intégrés aux deux autres sites Web d'ici mars 2023.

- *évalue les besoins en matière d'information et de fonctionnalité pour ensuite effectuer des analyses coûts-avantages lui permettant de déterminer s'il y a lieu à l'avenir de créer un nouveau site Web ou d'améliorer un site Web qui existe déjà.*
  État : En voie de mise en oeuvre d'ici mars 2023.

Détails

Lors de notre audit de 2020, nous avions constaté que trois des huit sites Web (metrolinx.com, metrolinxengage.com et thecrosstown.ca) offraient des renseignements semblables qui se recoupaient passablement, comme des renseignements organisationnels et des mises à jour sur la construction.

Lors de notre suivi, nous avons examiné le document d'approbation du projet de fusion des sites Web par le groupe d'investissement, daté du 13 avril 2021. Nous avons constaté qu'un fournisseur avait été choisi pour effectuer les travaux de développement visant à fusionner les sites Web existants, et qu'un avis d'attribution de marché avait été approuvé le 4 mars 2022. Nous avons examiné un calendrier d'élaboration faisant état des activités jusqu'en août 2022 et constaté que le fournisseur avait terminé plusieurs étapes du projet et qu'il était en voie, conformément à son calendrier, de mettre en ligne le premier site Web fusionné le 27 septembre 2022.

Recommandation 14

Pour améliorer la surveillance des projets de TI, ainsi que les pratiques de gestion des projets, de façon à ce que les projets de TI soient achevés à temps, conformément aux budgets estimatifs, nous recommandons que Metrolinx :

- *définisse clairement la portée des projets et fournisse les précisions nécessaires;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions observé de mauvaises pratiques de gestion et de surveillance des projets chez Metrolinx, ce qui avait entraîné des dépassements de coûts, des retards et des annulations.

Lors de l'examen que nous avions mené, nous avions constaté que le processus de gestion de projet de Metrolinx ne garantissait pas l'exécution des projets de TI à temps et conformément aux budgets approuvés.

Lors de notre suivi, nous avons constaté que tous les plans d'action découlant de cette recommandation avaient été mis en oeuvre par Metrolinx au moyen d'une nouvelle méthode de développement agile qui utilise une cible de livraison « à temps » de 90 %. Cette méthode d'élaboration exige la définition d'une portée claire pour le projet. Un mécanisme d'examen mensuel du projet a été mis en oeuvre pour examiner les projets dont l'état est « rouge » afin de s'assurer de cerner tout élément préoccupant. Nous avons examiné deux projets : la Stratégie de transformation numérique à l'intention de la clientèle et les projets de gestion de l'identité et de l'accès. Nous avons constaté que Metrolinx avait retenu et examiné une portée détaillée du projet lors des réunions du comité directeur, laquelle indique les jalons du projet, les risques et les dépendances des deux projets.

- *documente et surveille convenablement les échéanciers, les budgets et les coûts des projets;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions constaté que le processus de gestion de projet de Metrolinx ne garantissait pas l'exécution des projets de TI à temps et conformément aux budgets approuvés. Environ 72 % des projets de TI achevés avaient connu des dépassements de coûts combinés d'environ 152 millions de dollars, ce qui avait porté le coût total à 288 millions de dollars, un montant supérieur au double de celui de l'estimation initiale de 136 millions de dollars.

Dans notre suivi, outre l'examen mensuel des projets mentionné dans la recommandation précédente, nous avons constaté que Metrolinx présente des rapports mensuels sur les exceptions au groupe d'investissement pour tous les projets dont l'état est « rouge » ou « jaune ». Nous avons examiné les présentations soumises par Metrolinx au groupe d'investissement pour les deux projets échantillonnés et remarqué que Metrolinx inclut des budgets détaillés et des projections de coûts ventilés selon les exigences particulières, en plus d'indiquer si les travaux sont exécutés par un fournisseur ou par son personnel. La présentation indique également les dates des jalons clés à approuver, ainsi que toutes les dates des jalons précédentes tirées des présentations antérieures soumises au groupe d'investissement pour le même projet.

- *veille à superviser convenablement les changements apportés au projet, au moyen d'un motif bien documenté et des approbations pertinentes.*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2020, nous avions relevé des problèmes systémiques de gestion et d'exploitation des projets de TI, notamment un manque de surveillance des changements apportés aux projets.

Lors de notre suivi, nous avons constaté que les 10 projets les plus importants de Metrolinx ont été désignés aux fins d'un exercice d'essai de la nouvelle méthode de développement agile, qui a maintenant été étendue à tous les projets. De plus, un comité directeur a été mis sur pied pour examiner les changements qui sont apportés dans les projets clés. Nous avons examiné les documents de présentation destinés au comité directeur, pour chacun des deux projets échantillonnés: le système de gestion comptable des recettes et le système gestion de l'identité et de l'accès. Nous avons remarqué que les présentations comprenaient une ventilation détaillée des questions en suspens et de l'état d'avancement, ainsi qu'une feuille de route de l'état actuel des mesures prises et des mesures à prendre, assortie de dates clés associées à chaque étape. L'objet et les exigences clés du projet sont également énumérés, et les affectations budgétaires ont été utilisées jusqu'à maintenant pour s'assurer que les exigences du projet sont satisfaites en temps opportun et de façon rentable, et qu'elles respectent les spécifications énoncées dans la portée initiale du projet.