Chapitre 1

Section
1.13

Société des loteries et des jeux de l'Ontario

Systèmes technologiques (TI) et cybersécurité à la Société des loteries et des jeux de l'Ontario

Suivi des audits de l'optimisation des ressources, section 3.13 du *Rapport annuel 2019*

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 œuvre	Ne s'applique plus
Recommandation 1	1	1				
Recommandation 2	1	1				
Recommandation 3	2	2				
Recommandation 4	1	1				
Recommandation 5	1	1				
Recommandation 6	2	2				
Recommandation 7	2	2				
Recommandation 8	1	1				
Recommandation 9	3	3				
Recommandation 10	2			2		
Recommandation 11	1		1			
Recommandation 12	3	1		2		
Recommandation 13	1	1				
Recommandation 14	2		1	1		
Total	**23**	**16**	**2**	**5**	**0**	**0**
%	**100**	**69**	**9**	**22**	**0**	**0**

Conclusion globale

Au 30 juin 2021, la Société des loteries et des jeux de l'Ontario (OLG) avait pleinement mis en oeuvre 69 % des mesures que nous avions recommandées dans notre *Rapport annuel 2019*. OLG a réalisé des progrès dans la mise en œuvre de 9 % de nos recommandations.

OLG a pleinement mis en œuvre des recommandations comme l'examen régulier du rendement des fournisseurs grâce à l'établissement d'indicateurs de rendement pertinents, la surveillance du rendement conformément à ses ententes de niveau de service et la prise de mesures appropriées lorsque les cibles ne sont pas atteintes; la réalisation régulière de tests de pénétration de tous les systèmes de TI essentiels; l'examen et, au besoin, la mise à jour annuelle de sa définition et de sa classification des renseignements personnels; l'assurance que les données sont éliminées conformément aux exigences de la *Loi sur l'accès à l'information et la protection de la vie privée*; et la mise en œuvre d'un cadre de gestion de projet qui assure le suivi et la surveillance de tous les projets de TI ainsi que la production de rapports en temps opportun.

Parmi les recommandations qu'OLG était en train de mettre en œuvre, mentionnons l'examen de son code source de logiciel pour les systèmes de jeux électroniques et de TI des casinos, conformément aux pratiques exemplaires de l'industrie et la vérification périodique du rendement des exploitants de casinos quant à leurs responsabilités en matière de TI pour évaluer leur conformité aux exigences contractuelles et réglementaires.

OLG a fait peu de progrès en vue de la mise en oeuvre de 22 % des recommandations. Il s'agit notamment de recommandations liées à la cybersécurité et à la continuité de ses activités, ainsi qu'à l'examen officiel par la Division de la gestion des risques et de l'audit interne des rapports d'audits indépendants des casinos, y compris examiner et mettre à jour ses normes de sécurité de l'information pour préciser comment les casinos doivent protéger les renseignements personnels – par exemple, au moyen du chiffrement des renseignements personnels; veiller à ce que tous les casinos offrent leurs programmes de formation officiels à leur personnel pour réduire le risque de succès de cyberattaques; établir un plan complet de reprise après sinistre qui sera approuvé et mis à l'essai annuellement pour l'ensemble de son environnement de TI; examiner les rapports d'audits indépendants pour déterminer les risques de TI qui ont une incidence sur les activités opérationnelles d'OLG et confirmer que des mesures correctives ont été prises. La mise en œuvre de contrôles de cybersécurité robustes est plus importante que jamais pour prévenir et atténuer efficacement les menaces à la sécurité en réponse à l'augmentation des cyberattaques pendant la pandémie de COVID-19.

L'état des mesures prises pour donner suite à chacune de nos recommandations est décrit dans le présent rapport.

Contexte

La Société des loteries et des jeux de l'Ontario (OLG) est responsable de la direction et de la gestion de quatre secteurs d'activité : les jeux de loterie à l'échelle de la province (loteries), les jeux en ligne PlayOLG.ca (jeux en ligne), les centres de jeux de bienfaisance (jeux de bienfaisance) et 28 casinos en exploitation en Ontario.

OLG élabore et entretient les systèmes de TI pour ses jeux de loterie. Toutefois, les systèmes de TI pour les jeux en ligne et les casinos appartiennent à des fournisseurs de TI et sont utilisés par OLG conformément aux contrats de licence. OLG supervise les activités des jeux en ligne et des jeux de hasard ainsi que les casinos, mais les organismes sous contrat avec OLG (c'est-à-dire les exploitants de casinos) gèrent les activités quotidiennes des casinos.

Bien qu'OLG administre également le programme de financement du gouvernement de l'Ontario pour les courses de chevaux, les systèmes de TI utilisés expressément pour l'industrie des courses de chevaux sont exploités par des exploitants du secteur privé.

OLG est réglementée par la Commission des alcools et des jeux de l'Ontario, qui a fixé à 19 ans l'âge minimum pour le jeu et est chargée de tester l'intégrité des jeux d'OLG et de veiller à ce que les joueurs reçoivent un paiement équitable.

OLG a contribué environ 39 % du total des revenus non fiscaux de 5,9 milliards de dollars générés en 2019-2020 (45 % de 5,47 milliards de dollars en 2018-2019) par des entreprises publiques provinciales, comme la Régie des alcools de l'Ontario, Ontario Power Generation Incorporated, Hydro One Limited et l'Ontario Cannabis Retail Corporation.

Au cours des cinq dernières années, OLG a versé 728 millions de dollars à 68 fournisseurs de TI (651 millions de dollars à 68 fournisseurs de TI de 2013-2014 à 2018-2019) qui ont fourni des services de TI essentiels à l'appui de ses activités opérationnelles. Toute interruption des secteurs d'activité d'OLG aurait pu réduire les revenus de la province et avoir une incidence sur l'expérience des clients du jeu.

Nous avions notamment observé ce qui suit :

- OLG devait renforcer sa surveillance des fournisseurs de TI afin qu'ils fournissent des services et protègent les renseignements sur les clients plus efficacement et conformément aux attentes de rendement énoncées dans leurs contrats.
- OLG n'a pas examiné en profondeur le rendement des fournisseurs de TI au moment du renouvellement des contrats pour déterminer si chaque fournisseur avait satisfait aux attentes de rendement d'OLG en vertu de son contrat précédent.
- Bien qu'OLG ait effectué régulièrement des évaluations de la vulnérabilité, elle n'avait pas effectué régulièrement de tests de sécurité, comme des tests de pénétration pour ses secteurs d'activité des loteries et des jeux électroniques, afin de mieux cerner les vulnérabilités potentielles.
- Les renseignements personnels des clients d'OLG ont été chiffrés pour empêcher l'accès externe à ces renseignements; toutefois, sept employés d'OLG ont eu accès aux renseignements sous une forme non chiffrée, ce qui augmentait le risque que les renseignements personnels des clients soient lus à des fins inappropriées. Nous avons également constaté que deux casinos ne respectaient pas les normes de sécurité de l'information d'OLG et n'avaient pas chiffré les données sur les clients d'OLG dans leurs systèmes de TI.
- Il a été possible de renforcer les pratiques de cybersécurité dans les systèmes de TI utilisés dans les casinos, les loteries et les jeux en ligne. Par exemple, bien qu'OLG ait conclu un contrat avec un fournisseur de TI externe pour évaluer les contrôles techniques du générateur de nombres aléatoires pour son système de loterie et évalué la formule logicielle pour confirmer que le système était en mesure de générer des nombres aléatoires appropriés, nous avons constaté qu'OLG n'avait pas examiné le code source du logiciel pour déceler les lacunes en matière de cybersécurité en utilisant les pratiques exemplaires de l'industrie.
- OLG n'avait pas élaboré ni testé une stratégie globale de reprise après sinistre pour l'ensemble de son environnement de systèmes de TI. Bien que des stratégies de reprise après sinistre aient été élaborées et mises à l'essai pour les systèmes de TI de chaque secteur d'activité, nous avions constaté qu'OLG n'avait pas de stratégie globale intégrant tous les systèmes de TI de façon cohérente, même après un événement important qui aurait dû inciter OLG à en préparer un.
- OLG a lancé d'importants projets de TI dans divers secteurs d'activité. OLG avait mis en oeuvre 33 projets de TI dans les limites de son budget de 2013-2014 à 2018-2019, mais les 11 autres avaient dépassé le budget au cours des cinq dernières années (échantillon de 91 millions de dollars sur des dépenses totales de 232 millions dépensés), avec des retards et des dépassements de coûts de plus de 10 millions de dollars.

Nous avions formulé 14 recommandations comportant 23 mesures de suivi pour donner suite aux constatations de notre audit.

La Société des loteries et des jeux de l'Ontario s'était engagée à prendre des mesures pour donner suite à nos recommandations.

État des mesures prises en réponse aux recommandations

Nous avons effectué nos travaux de suivi entre mars et août 2021 pour la Société des loteries et des jeux de l'Ontario (OLG). Nous avons obtenu une déclaration écrite d'OPG selon laquelle, le 21 novembre 2021, l'entreprise avait fourni à notre Bureau une mise à jour complète sur l'état des recommandations que nous avions formulées dans notre audit initial, il y a deux ans.

OLG n'effectue pas toujours une surveillance et une évaluation approfondies du rendement des fournisseurs de TI, ce qui peut avoir une incidence sur l'expérience client

Recommandation 1

Pour améliorer la surveillance de la qualité des services de TI fournis, la Société des loteries et des jeux de l'Ontario doit établir des indicateurs et des cibles de rendement pertinents à intégrer à toutes les ententes sur les niveaux de service, surveiller le rendement par rapport aux cibles et, au besoin, prendre les mesures nécessaires pour répondre aux préoccupations.

État : Pleinement mise en œuvre.

Détails

Lors de notre audit de 2019, nous avions constaté qu'il était possible d'améliorer la surveillance exercée par la Société des loteries et des jeux de l'Ontario (OLG) sur ses fournisseurs de TI. Afin d'assurer la responsabilisation des fournisseurs et de veiller à ce que les attentes en matière de qualité des services des systèmes de TI soient bien comprises et respectées, des indicateurs de rendement – comme la disponibilité des services, la capacité du système et le temps de résolution des incidents de TI – doivent être inclus dans les contrats des fournisseurs. Nous avions constaté que trois des 10 contrats de fournisseurs de TI que nous avons examinés ne comportaient pas les indicateurs de rendement nécessaires dans leurs ententes sur les niveaux de service. OLG ne disposait donc pas d'un mécanisme contractuel pour surveiller la responsabilisation des fournisseurs à l'égard de la qualité du service.

Lors de notre suivi, nous avons constaté qu'en juillet 2020, OLG a mis à jour son processus normalisé de passation de marchés standard en intégrant un nouveau modèle de marché (intitulé « Entente de soutien et de niveau de service ») pour s'assurer que les indicateurs de rendement et les attentes ou les taux de réalisation appropriés, ainsi que l'intervalle de surveillance (c.-à-d. mensuel ou trimestriel), sont établis pour les services de TI fournis à OLG. En outre, OLG a renforcé sa division de l'approvisionnement afin de disposer de ressources compétentes pour améliorer la surveillance de la gestion de l'approvisionnement en TI, y compris l'élaboration des demandes de propositions et la négociation des exigences et des attentes des fournisseurs proposés.

Recommandation 2

Pour améliorer la surveillance des fournisseurs de TI, la Société des loteries et des jeux de l'Ontario doit examiner régulièrement le rendement des fournisseurs conformément à leurs ententes sur les niveaux de service et prendre les mesures qui s'imposent lorsque les objectifs ne sont pas atteints.

État : Pleinement mise en oeuvre.

Détails

Notre audit de 2019 avait révélé que les fournisseurs de trois systèmes de TI aux casinos – Omnigo (reconnaissance faciale), NRT (manipulation d'argent) et Avatar (prévention du blanchiment d'argent) – ne faisaient pas l'objet d'une surveillance efficace par OLG conformément à leurs ententes sur les niveaux de service. Par exemple, selon les ententes sur les niveaux de service, des réunions mensuelles et trimestrielles sur le rendement devraient avoir lieu

entre les gestionnaires d'OLG et les fournisseurs de TI. Nous avions constaté qu'OLG n'avait pas tenu de réunions avec ces fournisseurs ni obtenu de rapports de rendement pour savoir si les normes de service étaient respectées.

Lors de notre suivi, nous avons constaté qu'en mars 2020, OLG a mis en œuvre un cadre de classification des fournisseurs de TI et des fiches de notation comportant des objectifs de rendement pour gérer adéquatement les fournisseurs de technologie. De plus, OLG a examiné son processus de gestion par des tiers afin de fournir un document de recommandation qui lui permettra d'améliorer davantage le cadre global du processus de gestion des fournisseurs à l'échelle de l'entreprise. Nous avons également examiné le cadre de classification des fournisseurs de TI et les fiches de notation du rendement conformément à leurs ententes sur les niveaux de service, ainsi que la sélection de l'échantillon, et nous avons constaté qu'OLG avait établi des critères uniformes pour la classification des fournisseurs de TI ainsi que l'examen et le suivi du rendement des fournisseurs aux fins des mesures correctives. Voir les **recommandations 3** et **4** pour plus de détails.

Recommandation 3

Pour permettre la classification appropriée des fournisseurs de TI et faire en sorte que ceux-ci soient assujettis à un niveau de surveillance approprié, la Société des loteries et des jeux de l'Ontario doit :

- *établir des critères uniformes pour la classification des fournisseurs existants et nouveaux lorsqu'elle conclut des contrats avec eux, en utilisant des facteurs de sélection conformes aux pratiques exemplaires de l'industrie;*

  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2019, nous avions constaté que même si OLG compte trois catégories de fournisseurs (stratégiques, tactiques ou de produits) et des lignes directrices connexes, il n'existait pas d'approche uniforme pour déterminer la classification d'un fournisseur. Nous avions constaté que la classification était subjective et qu'elle était fondée sur la perception des fournisseurs par les responsables des activités de TI d'OLG. Par exemple, selon les catégories de fournisseurs et les lignes directrices, chaque fournisseur de TI qui a un contrat d'une valeur annuelle d'un million de dollars ou plus doit être classé dans la catégorie stratégique. Or, nous avions découvert que 13 des 51 fournisseurs classés dans la catégorie tactique (25 %) avaient reçu plus de 1 million de dollars par an au cours des 5 dernières années. Comme ces fournisseurs étaient classés dans la catégorie tactique, ils faisaient l'objet d'une surveillance moins étroite, c'est-à-dire que leur rendement était examiné chaque trimestre plutôt que chaque mois.

Lors de notre suivi, nous avons constaté qu'en décembre 2019, OLG a mis en œuvre un cadre de classification des fournisseurs de TI afin de bien classer et gérer les fournisseurs de technologies en fonction de l'importance des services qu'ils fournissent à OLG. Avant de mettre en œuvre le cadre de classification des fournisseurs de TI, OLG a analysé et intégré les pratiques exemplaires de l'industrie au cadre, y compris le modèle/trousse d'outils de segmentation des fournisseurs de Gartner et le guide IPPF de l'Institute of Internal Auditors. Nous avons également remarqué que les gestionnaires responsables de l'intégration des fournisseurs (ou de la TI) ont procédé à leur évaluation par catégorie (c.-à-d. risques financiers, importance de leurs activités pour la réputation d'OLG, taille de leurs contrats et type de services qu'ils fournissent aux opérations d'OLG) avec les critères de notation connexes afin d'assurer un processus d'examen uniforme.

- *examiner la classification des fournisseurs au moins une fois par année et lorsque des changements importants sont apportés à leurs activités.*

  État : Pleinement mise en oeuvre.

Détails

Notre audit de 2019 avait révélé qu'OLG n'examinait pas régulièrement les classifications des fournisseurs pour s'assurer que les fournisseurs de TI font l'objet d'une surveillance adéquate en fonction de leur classification.

Lors de notre suivi, nous avons constaté que les gestionnaires de l'intégration des fournisseurs ont examiné le cadre de classification des fournisseurs de TI afin de déterminer les changements à apporter aux fournisseurs de technologie existants ou à leurs gammes de services afin de s'assurer que la notation des fournisseurs repose sur les critères d'évaluation. OLG a terminé son premier examen annuel de la classification des fournisseurs en décembre 2020. Nous avons constaté que 43 des 163 fournisseurs de TI (26 %) avaient vu leur classification révisée par rapport à celle de décembre 2019 en fonction de l'examen effectué (c.-à-d. stratégique, tactique ou de produits) lors de l'examen annuel en décembre 2020.

Recommandation 4

Afin de confirmer en permanence l'importance pour les fournisseurs de TI de respecter leurs engagements contractuels en matière de rendement, la Société des loteries et des jeux de l'Ontario doit faire le suivi sur le rendement des fournisseurs et percevoir les paiements précisés dans les ententes sur les niveaux de service.

État : Pleinement mise en oeuvre.

Détails

Notre audit de 2019 avait révélé que quatre des 10 fournisseurs de TI que nous avions sélectionnés pour examen avaient une entente sur les niveaux de service contenant une clause qui les obligeaient à payer une pénalité à OLG si leurs services de TI n'étaient pas conformes à leur entente. Nous avions constaté que deux des quatre fournisseurs de notre échantillon n'avaient pas atteint leurs objectifs de rendement, mais OLG n'avait pas imposé le paiement de la pénalité. Si OLG n'applique pas cette exigence, ses fournisseurs peuvent être moins incités à atteindre leurs objectifs de rendement.

Lors de notre suivi, nous avons constaté qu'OLG avait défini et intégré les mesures de rendement des fournisseurs (IRC) aux fiches de notation pour assurer une surveillance régulière du rendement stratégique des fournisseurs et produire des rapports à ce sujet. OLG a également mis à jour ses procédures existantes pour percevoir les crédits de service ou les pénalités des fournisseurs dont les contrats incluaient des clauses de pénalité. Lorsque les objectifs de rendement de l'entente de niveau de service (ENS) définie dans le contrat visé ne sont pas atteints, le fournisseur doit accorder des crédits de service ou payer une pénalité conformément à ses obligations contractuelles. De plus, OLG a mis en œuvre un processus de gestion des fournisseurs de TI (GFT) et un programme de formation qui décrivent les rôles et les responsabilités du gestionnaire de l'intégration des fournisseurs afin d'assurer une surveillance uniforme des divers fournisseurs de TI.

Recommandation 5

Pour disposer d'un remplaçant fiable pour son fournisseur d'accès Internet principal qui lui permettra d'assurer la continuité de ses activités opérationnelles, la Société des loteries et des jeux de l'Ontario doit analyser les coûts et les avantages liés au recours à un fournisseur secondaire d'accès Internet.

État : Pleinement mise en oeuvre.

Détails

Notre audit de 2019 avait révélé que Rogers Communications était le seul fournisseur d'accès Internet pour tous les détaillants de produits de loterie de l'Ontario et le principal fournisseur d'accès Internet d'OLG. Si Rogers subissait une panne à l'échelle de la province, OLG n'aurait pas de fournisseur de remplacement pour soutenir ses activités quotidiennes.

Lors de notre suivi, nous avons constaté qu'OLG avait effectué une évaluation pour analyser les coûts et les avantages associés à l'acquisition d'un fournisseur secondaire d'accès Internet afin d'améliorer la continuité de ses activités opérationnelles et de réduire au minimum l'incidence

des pannes de réseau. Nous avons remarqué qu'OLG a effectué une analyse des tendances des quatre dernières années (de 2017 à 2020) en ce qui concerne la disponibilité du réseau des détaillants et les délais de réparation des pannes. À la lumière de l'analyse d'OLG, nous avons constaté que les incidents aux points de vente au détail avaient été réduits à moins de deux fois par point de vente en 2020 et que les objectifs de l'entente sur les niveaux de service (ENS) pour la disponibilité du réseau et le temps requis pour réparer les pannes aux points de vente au détail avaient été atteints en 2020. En outre, OLG a analysé les répercussions possibles sur les revenus de loterie en raison de pannes pour la même période. Compte tenu des coûts supplémentaires importants liés à un fournisseur de réseau secondaire, OLG a conclu que le coût dépasserait les avantages potentiels. En outre, OLG a effectué une étude comparative d'autres sociétés de loterie régionales au Canada et a appris qu'elles n'avaient pas recours à un fournisseur de réseau secondaire pour les détaillants de loterie.

Recommandation 6

Pour améliorer la surveillance des fournisseurs de TI, la Société des loteries et des jeux de l'Ontario doit, avant de prolonger ou de renouveler un contrat existant :

- *effectuer des évaluations approfondies du rendement de ses fournisseurs actuels;*
  État : Pleinement mise en oeuvre.

Détails

Lors de notre audit de 2019, nous avions constaté qu'OLG avait prolongé les contrats de TI de 4 des 10 fournisseurs de TI que nous avons examinés, les paiements cumulatifs allant de 1,5 à 23,2 millions de dollars, sans évaluer leur rendement en profondeur. Pour assurer une gouvernance efficace de l'approvisionnement et des contrats de TI, l'organisme superviseur doit évaluer le rendement des fournisseurs – au moyen d'outils comme les fiches de rendement, les rapports sur la qualité des services et des produits, les registres des problèmes et les cotes de risque – avant de renouveler les principaux contrats de TI. Ces évaluations donnent aux organismes l'assurance que les fournisseurs ont fourni les biens et services conformément aux ententes.

Lors de notre suivi, nous avons constaté qu'OLG avait amélioré le processus de renouvellement des contrats des fournisseurs de TI en révisant les procédures de gestion du renouvellement ainsi que les rôles et responsabilités des principaux intervenants, en veillant à ce que l'évaluation du rendement des fournisseurs soit effectuée régulièrement et en offrant une formation sur l'approvisionnement aux principaux intervenants, comme les responsables des contrats, les gestionnaires de l'intégration des fournisseurs et les spécialistes de l'approvisionnement. Voir la **recommandation 4** pour plus de détails. De plus, OLG a mis en œuvre une nouvelle fonction liée aux activités de gestion du renouvellement dans le système de TI de gestion des contrats (ContractHub) pour permettre aux responsables de l'approvisionnement d'entreprendre des activités de renouvellement avec les responsables des contrats, y compris l'évaluation des contrats actifs et la saisie des examens du rendement des fournisseurs auprès des unités opérationnelles.

- *améliorer le processus actuel d'approvisionnement, en déterminant s'il est plus approprié de lancer un nouvel appel d'offres que de prolonger ou de renouveler ses contrats.*
  État : Pleinement mise en œuvre.

Détails

Lors de notre suivi, nous avons constaté qu'OLG avait amélioré le processus actuel d'approvisionnement afin qu'il exige maintenant une analyse de rentabilisation (analyse coûts-avantages) pour déterminer si un nouvel appel d'offres de service est plus approprié que la prolongation ou le renouvellement du contrat existant. Nous avons examiné un échantillon d'une évaluation effectuée pour le logiciel actuel qui offre un service à OLG afin qu'il puisse partager des fichiers en toute sécurité avec des parties externes. D'après l'évaluation effectuée par l'équipe de prestation des solutions de TI d'OLG, nous avons

constaté que l'équipe des TI d'OLG avait été avisée d'explorer, dans le cadre de son analyse des coûts et des avantages, d'autres options à la lumière de l'évaluation de la solution. Par conséquent, l'équipe des TI d'OLG a décidé de tirer parti du système actuel qui est doté d'une capacité de partage de fichiers au lieu de renouveler le contrat.

Recommandation 7

Pour renforcer la surveillance des fournisseurs de TI, la Société des loteries et des jeux de l'Ontario (OLG) doit :

- *préciser et communiquer à ses gestionnaires de TI leurs rôles et responsabilités en matière de surveillance de la conformité des fournisseurs aux engagements contractuels énoncés dans les ententes sur les niveaux de service;*
  État : Pleinement mise en œuvre.

Détails

Lors de notre audit de 2019, nous avions constaté que les réunions sur le rendement n'avaient pas lieu comme l'exigent les contrats. Les 10 gestionnaires que nous avons interviewés nous avaient dit que leurs rôles et responsabilités n'étaient pas bien définis et que les exigences de leur poste à cet égard n'étaient pas claires. Leurs responsabilités devaient être précisées pour s'assurer qu'ils tiennent des réunions sur le rendement (par téléphone ou en personne), comme l'exigent les contrats des fournisseurs.

Lors de notre suivi, nous avons constaté qu'OLG avait mis en œuvre un processus de gestion des fournisseurs de technologie (GFT) et un programme de formation qui décrivent les rôles et les responsabilités du gestionnaire de l'intégration des fournisseurs et fournissent des lignes directrices pour la mise en œuvre uniforme du processus de GBT. Le processus de GFT comprend des responsabilités détaillées pour les gestionnaires des fournisseurs, comme la gestion des obligations contractuelles et des ententes de niveau de service en matière de technologie, le suivi régulier des relations avec les fournisseurs et des objectifs de rendement, et la gestion des risques (p. ex., évaluations des menaces et des risques) afin de gérer efficacement le rendement des fournisseurs.

- *élaborer des directives à l'intention de ses gestionnaires sur ce qui constitue une surveillance efficace du rendement des fournisseurs.*
  État : Pleinement mise en œuvre.

Détails

Notre audit de 2019 avait révélé que les renseignements sur les fournisseurs, comme les contrats antérieurs et les activités des fournisseurs, les procès-verbaux de réunions et les rapports de rendement, ne sont pas sauvegardés dans le répertoire central des TI ou ne sont pas facilement accessibles. Par conséquent, nous avions constaté que les gestionnaires d'OLG ne disposaient pas de renseignements clés sur les tendances et activités antérieures liées au rendement des fournisseurs.

Lors de notre suivi, nous avons constaté qu'OLG avait élaboré et mis en œuvre des ressources de formation sur la gestion des fournisseurs dans le système de formation ministériel et que tous les gestionnaires de l'intégration des fournisseurs devaient suivre cette formation. Nous avons constaté qu'OLG avait obtenu une attestation annuelle des 52 gestionnaires des TI affirmant qu'ils avaient terminé la formation en date du 1er juin 2021.

La sécurité des renseignements personnels des clients et des employés d'OLG peut être renforcée

Recommandation 8

Pour se protéger plus efficacement contre le risque de cyberattaques, protéger les renseignements personnels et assurer la continuité des services, la Société des loteries et des jeux de l'Ontario (OLG) doit effectuer des tests de pénétration réguliers de tous ses systèmes de TI critiques.
État : Pleinement mise en œuvre.

Détails

Lors de notre audit de 2019, nous avions constaté qu'OLG effectuait régulièrement des évaluations de la vulnérabilité, mais qu'elle n'effectuait pas régulièrement de tests de pénétration afin de mieux cerner les vulnérabilités en matière de cybersécurité. Ainsi, nous avions remarqué que son site Web de jeux électroniques, PlayOLG.ca, n'avait pas été testé régulièrement depuis son lancement en janvier 2015. Nous avions constaté que les derniers tests remontaient à 2016 et à 2017. De plus, OLG n'avait pas effectué de test de pénétration de l'application mobile de loterie OLG, qui a été mise au point par un fournisseur de TI et qui stocke les renseignements personnels des clients. Une violation potentielle de l'application accroît le risque que les données des clients, y compris leurs noms, adresses et numéros de téléphone, soient compromises.

Depuis notre audit, nous avons constaté qu'en juin 2020, OLG a établi une politique de sécurité pour les tests de pénétration afin d'évaluer la vulnérabilité des systèmes. La politique énonce les critères, la portée et l'échéancier de l'évaluation, les rapports et analyses techniques ainsi que les mesures d'atténuation et les nouveaux tests nécessaires pour les tests réguliers des systèmes de TI essentiels d'OLG. Nous avons constaté qu'OLG a effectué des tests de pénétration du site Web de jeux en ligne PlayOLG.ca en août 2020 et en avril 2021, et de l'application mobile de loterie d'OLG en février 2020 et en avril 2021.

Recommandation 9

Pour protéger les renseignements personnels contre les atteintes à la vie privée, la Société des loteries et des jeux de l'Ontario doit :

- *chiffrer tous les renseignements personnels et en restreindre l'accès en utilisant les pratiques exemplaires de l'industrie;*
  État : Pleinement mise en œuvre.

Détails

Notre audit de 2019 avait révélé qu'OLG recueillait les renseignements personnels des clients à des fins commerciales et pour se conformer à la réglementation. Les renseignements sont sauvegardés dans les bases de données d'OLG et chiffrés pour empêcher les attaquants d'y accéder. Au moment de notre audit, nous avions toutefois constaté qu'OLG comptait sept employés qui avaient un accès illimité aux bases de données contenant tous les renseignements confidentiels de ses clients. Cela n'est pas conforme aux pratiques exemplaires en matière de sécurité. Les pratiques exemplaires exigeraient un compte privilégié du système (comme un identifiant Firecall) plutôt que ces sept comptes privilégiés individuels. Un « identifiant Firecall » est une méthode établie pour fournir un accès temporaire et surveillé à des renseignements de nature délicate et sécurisés.

Lors de notre suivi, nous avons constaté que la politique de protection des données d'OLG prévoit que les fonds de renseignements de nature délicate, y compris les renseignements personnels, doivent être protégés contre toute divulgation non intentionnelle en utilisant des techniques de chiffrement qui protégeront les renseignements au fur et à mesure qu'ils sont sauvegardés, communiqués ou utilisés. Nous avons remarqué qu'OLG chiffrait tous les renseignements personnels stockés dans les systèmes conformes au champ d'application comme nous l'avions recommandé dans notre audit de 2019 et qu'elle avait mis en œuvre des contrôles de sécurité comme le contrôle de l'accès des utilisateurs et du réseau pour surveiller et consigner l'accès à ces renseignements par les administrateurs des bases de données privilégiés.

- *examiner et, au besoin, mettre à jour annuellement sa définition et sa classification des renseignements personnels;*
  État : Pleinement mise en œuvre.

Détails

Lors de notre audit de 2019, nous avions également constaté qu'OLG avait une définition trop étroite des données personnelles, de sorte que les renseignements personnels recueillis dans les casinos qui ne correspondent pas à cette définition étroite n'étaient pas protégés dans la même mesure que les renseignements personnels qui répondent à la définition. Par exemple, OLG utilise les systèmes de TI des casinos pour identifier les joueurs à accès restreint : le système de TI saisit leurs images dans des photos et les compare à une base de données sur les joueurs à accès restreint. Ces photos sont converties en formules mathématiques qui ne sont pas classées comme des renseignements personnels par OLG. Toutefois, le commissaire à l'information et à la protection de la vie privée de l'Ontario nous a informés que ces formules mathématiques décrivant la géométrie faciale d'une personne devraient être considérées comme des renseignements personnels.

Lors de notre suivi, nous avons constaté qu'OLG avait mis en œuvre une politique sur la protection des renseignements personnels en avril 2020. La politique décrit la définition et la classification des renseignements personnels et le signalement des atteintes à la vie privée et des problèmes connexes, ainsi que les rôles et les responsabilités des principaux intervenants d'OLG. La politique sur la protection des renseignements personnels précise que la définition des renseignements personnels doit être revue annuellement. Nous avons également remarqué qu'OLG avait informé son personnel de la mise en oeuvre de la nouvelle politique, en mettant l'accent sur la responsabilité des employés de se conformer aux exigences de la politique sur la protection des renseignements personnels.

- *veiller à la disposition des données conformément aux exigences de la* Loi sur l'accès à l'information et la protection de la vie privée.
  État : Pleinement mise en œuvre.

Détails

Lors de notre audit de 2019, nous avions constaté que les renseignements personnels des clients d'OLG tombent sous le coup de la *Loi sur l'accès à l'information et la protection de la vie privée* (la Loi) de l'Ontario. Aux termes de la Loi, OLG doit tenir un registre indiquant les types de données personnelles dont elle dispose et la date de leur disposition. Nous avions toutefois constaté que la Division des TI d'OLG ne tenait pas un tel registre pour la disposition des renseignements personnels des joueurs de loterie et des clients des casinos.

Lors de notre suivi, nous avons constaté qu'OLG avait mis à jour le système d'archivage afin qu'il conserve maintenant des dossiers sur les types de données personnelles et la date de leur disposition. OLG a également offert une formation aux membres du personnel qui ont la garde des données personnelles pour les sensibiliser à leurs responsabilités, y compris aux exigences de conformité à la *Loi sur l'accès à l'information et la protection de la vie privée*. Nous avons examiné les registres de disposition de données de janvier à février 2021 et constaté qu'OLG avait consigné la date, le numéro d'identification de l'incident, le type de données, les personnes qui en ont demandé la suppression et la raison de la disposition des données personnelles.

Recommandation 10

Pour se conformer à ses propres normes, la Société des loteries et des jeux de l'Ontario (OLG) doit :

- *examiner et mettre à jour ses normes de sécurité de l'information afin de préciser comment les casinos doivent protéger les renseignements personnels, par exemple en les chiffrant;*
  État : Peu ou pas de progrès.

Détails

Lors de notre audit de 2019, nous avions constaté que les casinos sont tenus par contrat de sauvegarder les renseignements sur les clients d'OLG, conformément aux normes de sécurité de l'information

d'OLG. Toutefois, nous avions constaté que les normes indiquent seulement que les casinos doivent protéger l'information, mais ne précisent pas comment cela doit être fait. Lors de notre visite à deux casinos, nous avions constaté que ni l'un ni l'autre ne chiffrait les données des clients d'OLG dans ses systèmes de TI.

Au moment de notre suivi, nous avons constaté qu'OLG n'avait pas pris de mesures suffisantes pour s'assurer que les exploitants de casinos protègent les renseignements personnels en mettant en oeuvre des mesures de protection comme le chiffrement. OLG nous a informés qu'en raison de la pandémie de COVID-19, les casinos ontariens sont fermés depuis mars 2020. Par conséquent, les casinos disposent d'un nombre restreint d'employés pour soutenir leurs activités, ce qui entraîne des retards dans la mise en œuvre du chiffrement des données personnelles. OLG collaborera avec chaque exploitant de casino pour dresser une feuille de route d'ici le 30 juin 2022, afin d'assurer la pleine conformité aux exigences de chiffrement des renseignements personnels.

- *veiller à ce que tous les casinos offrent ses programmes de formation structurés à leur personnel afin de réduire le risque de cyberattaques réussies.*

  État : Peu ou pas de progrès.

Détails

Lors de notre audit de 2019, nous avions constaté qu'une atteinte à la protection des données s'était produite en novembre 2016, lorsque Casino A a été victime d'une cyberattaque au cours de laquelle des données de nature délicate sur les clients et les employés du casino ont été volées. OLG et le Commissariat à l'information et à la protection de la vie privée de l'Ontario avaient indiqué que l'incident était attribuable à un courriel d'hameçonnage envoyé aux employés de Casino A, qui a entraîné le vol d'environ 14 000 dossiers, y compris des rapports financiers, des demandes de crédit des clients, des renseignements sur le recouvrement des dettes, ainsi que des données sur la paie et d'autres données. À la suite de l'incident au Casino A, OLG avait renforcé les dispositions dans les ententes avec les exploitants des casinos pour s'assurer que les atteintes à la protection des données étaient traitées et signalées conformément à ses pratiques de sécurité de l'information. Toutefois, OLG n'avait pas confirmé que les casinos avaient fourni des directives à leurs employés sur une base continue pour prévenir un incident semblable. Nous avions également remarqué que deux autres attaques d'hameçonnage avaient eu lieu depuis. Ces deux incidents étaient semblables à celui survenu au Casino A, où l'incident aurait pu être évité si les employés avaient reconnu les courriels suspects.

Au moment de notre suivi, nous avons constaté qu'OLG avait fait peu ou pas de progrès pour s'assurer que tous les exploitants de casinos offrent une formation annuelle de sensibilisation sur la sécurité de l'information à leur personnel. Cette mesure a été retardée en raison de la fermeture des casinos ontariens et du nombre restreint d'employés des casinos pour soutenir les activités pendant la pandémie de COVID-19. OLG a rédigé des lignes directrices de base pour un programme de sensibilisation à la sécurité de l'information afin de préciser et de renforcer les exigences particulières que doivent respecter les exploitants de casinos. OLG communiquera les exigences aux exploitants de casinos d'ici le 30 octobre 2021 et prévoit mettre en œuvre la recommandation d'ici le 30 juin 2022.

D'autres mesures pourraient être prises pour réduire davantage les risques liés à la cybersécurité pour les systèmes de loterie, de casino et de jeux en ligne

Recommandation 11

Pour améliorer la sécurité lors de la génération de numéros de loterie et cerner les lacunes en matière de cybersécurité des systèmes de TI des jeux en ligne et des casinos, la Société des loteries et des jeux de l'Ontario doit examiner le code source de son logiciel conformément aux pratiques exemplaires de l'industrie.

État : En voie de mise en oeuvre d'ici décembre 2021.

Détails

Lors de notre audit de 2019, nous avions constaté que l'équipe des TI d'OLG n'examinait pas le code source du logiciel des systèmes de TI critiques utilisés pour ses opérations de loterie, de jeux en ligne et de casino. Le code source des logiciels contient des instructions rédigées par un programmeur qui peuvent être lues par des humains. Bien que le code source des logiciels des jeux en ligne et des casinos est examiné par le fournisseur qui appuie ces systèmes, OLG ne suivait pas la pratique exemplaire de l'industrie qui consiste à repérer les lacunes en matière de cybersécurité, soit en exécutant un examen indépendant du code source des logiciels ou en s'assurant que les fournisseurs effectuent de tels examens avec diligence.

Lors de notre suivi, nous avons constaté qu'OLG avait mis à jour le processus lié au cycle de vie d'élaboration des systèmes (CVES) pour rendre obligatoire l'examen des codes sources. OLG met actuellement la dernière main à la politique sur le code source du logiciel afin de définir les exigences d'examen du code source et choisit un outil logiciel pour satisfaire aux exigences de cet examen. OLG prévoit parachever et mettre en œuvre la politique avec l'outil d'analyse logicielle d'ici le 31 décembre 2021.

Une stratégie complète de reprise après sinistre et de mise à l'essai est nécessaire

Recommandation 12

Pour gérer les risques pour ses principaux systèmes de TI, la Société des loteries et des jeux de l'Ontario (OLG) doit :

- *établir un plan complet de reprise après sinistre à faire approuver et à mettre à l'essai annuellement pour l'ensemble de son environnement de TI;*
  État : Peu ou pas de progrès.

Détails

Lors de notre audit de 2019, nous avions constaté qu'OLG n'avait pas de plan complet de reprise après sinistre intégrant tous les systèmes de TI de façon cohérente. Cela est devenu évident lorsqu'OLG a connu une panne majeure de près de six heures le 29 octobre 2018, qui a interrompu l'accès aux systèmes de TI clés comme le système de loterie et le système de gestion des jeux. Nous avions appris qu'un commutateur de réseau au centre de données de Toronto était tombé en panne à 12 h 47 et que les services n'avaient été rétablis que près de six heures plus tard, à 6 h 38. Au moment de notre audit, OLG n'avait pas encore élaboré ni mis à l'essai une stratégie globale de reprise après sinistre qui lui permettrait de reprendre ses activités dans les délais cibles.

Lors de notre suivi, nous avons constaté qu'OLG avait retenu les services d'un fournisseur tiers et procédé à un examen de la résilience de la technologie stratégique pour intégrer les recommandations à l'établissement d'un plan complet de reprise après sinistre. En avril 2021, OLG a mis sur pied le groupe de travail sur le plan de reprise après sinistre et prévoit mettre celui-ci en œuvre d'ici le 31 décembre 2022.

- *examiner périodiquement la classification des systèmes de TI d'OLG et des casinos pour en assurer l'uniformité;*
  État : Peu ou pas de progrès.

Détails

Nous avions constaté dans notre audit de 2019 qu'OLG classe ses 186 systèmes en fonction de leur importance pour ses activités opérationnelles. Les classifications déterminent si un test de reprise après sinistre est nécessaire et, dans l'affirmative, la fréquence des tests et la rapidité avec laquelle OLG devrait être en mesure d'accéder à nouveau à ces systèmes. Nous avions remarqué qu'OLG n'avait pas examiné les classifications de ses systèmes pour s'assurer qu'elles permettaient de respecter le délai de rétablissement cible.

Lors de notre suivi, nous avons constaté qu'OLG avait fait peu ou pas de progrès dans l'examen périodique de la classification de ses systèmes d'information pour en assurer l'uniformité à l'échelle de ses systèmes de TI et des casinos. OLG prévoit mettre en œuvre cette recommandation d'ici le 31 décembre 2021.

- *tester de nouveau le plan de reprise après sinistre de ses systèmes de TI après chaque échec.*
  État : Pleinement mise en œuvre.

Détails

Lors de notre suivi, nous avons constaté qu'OLG avait mis en œuvre un processus de suivi des tests du plan de reprise après sinistre pour ses systèmes de TI en décembre 2020. Ce processus permet également de s'assurer que lorsqu'un test du plan de reprise après sinistre échoue, par exemple, il n'atteint pas le délai cible de reprise en moins de quatre heures ou dans les 24 heures selon l'importance de ces systèmes de TI pour les opérations d'OLG, des mesures correctives sont prises pour se pencher sur les raisons de la défaillance. Une fois les mesures correctives prises, OLG prévoit et refait les tests non réussis de plans de reprise après sinistre pour s'assurer qu'ils obtiennent des résultats satisfaisants.

Certains projets de TI ont connu des retards de mise en oeuvre et des dépassements de coûts d'environ 10 millions de dollars

Recommandation 13

Afin d'appliquer sa stratégie numérique avec succès et d'éviter le risque de retards dans la mise en œuvre et de dépassements de coûts, la Société des loteries et des jeux de l'Ontario doit mettre en oeuvre un cadre de gestion de projet qui assure le suivi et la surveillance de tous les projets de TI et en fait rapport en temps opportun.

État : Pleinement mise en œuvre.

Détails

Lors de notre audit de 2019, nous avions constaté qu'OLG avait mis en œuvre 44 projets de TI à un coût de 232 millions de dollars dans ses divers secteurs d'activité, comme la mise en place du site Web de jeu en ligne PlayOLG.ca et de l'application mobile de loterie OLG, et elle a mis à niveau les systèmes de TI clés dans les casinos et les sites de jeu de bienfaisance. OLG avait mis en œuvre 33 projets de TI dans les limites de son budget. Toutefois, les 11 autres projets, qui représentaient environ la moitié du total des dépenses liées aux projets de TI au cours des cinq dernières années (échantillon de 91 millions de dollars sur des dépenses totales de 232 millions) affichaient des retards et des dépassements de coûts de plus de 10 millions de dollars. Nous avions remarqué que de nombreux facteurs contribuaient aux retards et aux dépassements de coûts, notamment une surveillance plus faible des projets.

Lors de notre suivi, nous avons constaté qu'en janvier 2020, OLG avait mis en œuvre un nouveau cadre de contrôle des projets pour renforcer la surveillance et assurer le suivi, la surveillance et la production de rapports sur les projets de TI en temps opportun. Nous avons examiné l'exemple de projet de TI et les soutiens correspondants. Nous avons constaté que l'analyse de rentabilisation, la charte du projet, le plan de mise en œuvre du projet, la demande de changement au projet et les rapports d'étape hebdomadaires pour gérer la mise en œuvre du projet ainsi que l'examen postérieur au projet étaient conformes au nouveau cadre de contrôle du projet. OLG a également offert une formation sur la gouvernance de projet au personnel du Bureau de gestion de projet et aux principaux intervenants de la technologie et des finances afin qu'ils comprennent le nouveau cadre de gestion de projet et leurs responsabilités.

La Division de la gestion des risques et de l'audit interne d'OLG n'effectue pas d'audits indépendants des casinos pour réduire les risques liés aux TI

Recommandation 14

Pour améliorer l'efficacité de la surveillance des opérations de TI dans les casinos, la Division de la gestion des risques et de l'audit interne de la Société des loteries et des jeux de l'Ontario (OLG) doit :

- *vérifier périodiquement si les exploitants de casinos s'acquittent de leurs responsabilités en matière de TI afin d'évaluer leur conformité aux exigences contractuelles et réglementaires;*
  État : En voie de mise en oeuvre d'ici mars 2023.

Détails

Lors de notre audit de 2019, nous avions constaté que la Division de la gestion des risques et de l'audit interne d'OLG n'avait pas effectué des audits indépendants des TI dans tous les casinos, comme le permettent les ententes. La Division de la gestion des risques et de l'audit interne n'avait effectué que 15 audits des TI pour les 26 casinos, et ces audits avaient une portée limitée. Cela ne donne pas une assurance suffisante que les casinos se conforment à leurs responsabilités en matière de TI conformément aux ententes.

Au moment de notre suivi, nous avons constaté qu'OLG avait élaboré un plan d'audit interne visant à fournir une assurance sur les contrôles de TI des exploitants de casinos pour faire en sorte que tous les exploitants de casinos soient assujettis à un examen dans le cadre d'un cycle triennal d'avril 2020 à mars 2023. Le plan d'audit définit également la portée de l'audit des TI, comme le contrôle de l'accès des utilisateurs, la gestion des vulnérabilités en matière de sécurité, la protection des données et les programmes de sensibilisation à la sécurité de l'information des utilisateurs.

Nous avons constaté que la Division des risques et de l'audit d'OLG avait effectué l'audit des TI portant sur 11 casinos sur 28 (39 %) en 2021.

- *examiner formellement les rapports d'audit externe pour cerner les risques informatiques qui ont une incidence sur les activités opérationnelles d'OLG et confirmer que des mesures correctives ont été prises.*
  État : Peu ou pas de progrès.

Détails

Lors de notre audit de 2019, nous avions également constaté que, dans les cas où les audits des casinos étaient effectués par les auditeurs externes, la Division de la gestion des risques et de l'audit interne d'OLG n'examinait pas les rapports d'audit pour déterminer si les audits avaient mis au jour des lacunes systémiques et des risques pour les activités de TI qui ont une incidence sur OLG. Nous avions examiné ces rapports et constaté que les rapports d'audit faisaient état de lacunes telles que des préoccupations relatives à l'accès des utilisateurs et la faiblesse des contrôles de sécurité pour les systèmes clés.

Depuis notre audit, la Division de la gestion des risques et de l'audit interne d'OLG a fait peu de progrès dans l'examen des risques de TI relevés par les auditeurs externes des exploitants de casinos pour évaluer l'incidence sur les activités d'OLG et confirmer que des mesures correctives ont été prises. Nous avons remarqué que le rapport d'audit externe des TI effectué par les auditeurs externes d'OLG (KPMG) à l'exercice 2019-2020 avait été examiné, mais que les plans correctifs n'avaient pas été entièrement mis en œuvre par les exploitants de casinos. Nous avons également remarqué qu'OLG avait reçu six rapports d'audit des TI effectués par les auditeurs des exploitants de casinos au cours de l'exercice 2020-2021. Bien qu'OLG examine et assure le suivi des constatations des rapports d'audit des TI des exploitants de casinos, nous avons constaté qu'OLG n'avait pas effectué d'évaluation officielle

pour déterminer les risques de TI ayant une incidence sur ses activités opérationnelles.

De plus, nous avons constaté que deux exploitants de casinos (Hard Rock Ottawa et Caesars Entertainment) n'avaient fourni aucun rapport d'audit des TI au cours de l'exercice 2020-2021 aux fins de l'examen officiel d'OLG.