Chapter 1
Section
1.13

Ontario Lottery and Gaming Corporation

Technology Systems (IT) and Cybersecurity at Ontario Lottery and Gaming Corporation

Follow-Up on VFM Section 3.13, *2019 Annual Report*

RECOMMENDATION STATUS OVERVIEW

		Status of Actions Recommended				
	# of Actions Recommended	Fully Implemented	In the Process of Being Implemented	Little or No Progress	Will Not Be Implemented	No Longer Applicable
Recommendation 1	1	1				
Recommendation 2	1	1				
Recommendation 3	2	2				
Recommendation 4	1	1				
Recommendation 5	1	1				
Recommendation 6	2	2				
Recommendation 7	2	2				
Recommendation 8	1	1				
Recommendation 9	3	3				
Recommendation 10	2			2		
Recommendation 11	1		1			
Recommendation 12	3	1		2		
Recommendation 13	1	1				
Recommendation 14	2		1	1		
Total	**23**	**16**	**2**	**5**	**0**	**0**
%	**100**	**69**	**9**	**22**	**0**	**0**

Overall Conclusion

The Ontario Lottery and Gaming Corporation (OLG), as of June 30, 2021, has fully implemented 69% of the actions we recommended in our *2019 Annual Report*. OLG has made progress in implementing an additional 9% of our recommendations.

OLG has fully implemented recommendations such as reviewing vendors' performance regularly by establishing appropriate performance indicators, monitoring performance in accordance with their service-level agreements and taking appropriate action when targets are not met; regularly performing penetration testing of all critical IT systems; reviewing

and where needed updating its definition and classification of personal information annually; ensuring that data is disposed of according to the requirements of the *Freedom of Information and Protection of Privacy Act*; and implementing a project management framework that tracks, monitors and reports on all IT projects on a timely basis.

Recommendations that OLG was in the process of implementing include reviewing its software source code for the iGaming and casino IT systems in accordance with industry best practices and auditing casino operators' performance of their IT responsibilities on a periodic basis to assess their compliance with contractual and regulatory requirements.

OLG has made little progress on 22% of the recommendations. These include recommendations related to cybersecurity and continuity of its operations, and to its Internal Risk and Audit Division's formal review of external audit reports of casinos, including reviewing and updating its information security standards to specify how casinos are to protect personal information—for example, with encryption of personal information; ensuring that all casinos deliver their established formal training programs for their staff to reduce the risk of successful cyberattacks; establishing a comprehensive disaster recovery plan to be approved and tested on an annual basis for its entire IT environment; and reviewing external audit reports to identify IT risks impacting OLG's business operations and confirming that corrective action has been taken. Implementing robust cybersecurity controls is more critical than ever to prevent and mitigate security threats in an efficient manner in response to increasing cyberattacks during the COVID-19 pandemic.

The status of actions taken on each of our recommendations is described in this report.

Background

The Ontario Lottery and Gaming Corporation (OLG) is responsible for conducting and managing the following four lines of business: province-wide lottery games (lottery), PlayOLG.ca Internet gaming (iGaming), charitable gaming centres (cGaming), and 28 casinos operating in Ontario.

OLG develops and maintains the IT systems for its lottery games. However, IT systems for iGaming, cGaming and casinos are owned by IT vendors and used by OLG in accordance with licensing agreements. OLG oversees the operations of iGaming and cGaming and also oversees the casinos, but organizations under contract to OLG (that is, casino operators) manage the casinos' day-to-day operations.

Although OLG also administers the Ontario government's funding program for horse racing, the IT systems specifically used for the horse-racing industry are operated by private-sector operators.

OLG is regulated by the Alcohol and Gaming Commission of Ontario, which has set the minimum age for gambling at 19 and is responsible for testing the design of OLG's games for the games' integrity and ensuring that players receive a fair payout.

OLG contributed about 39% of the total $5.9 billion in non-tax revenue generated in 2019/20 (45% of $5.47 billion in 2018/19) by provincial government business enterprises, such as the Liquor Control Board of Ontario, Ontario Power Generation Incorporated, Hydro One Limited and the Ontario Cannabis Retail Corporation.

In the past five years, OLG paid $728 million to 68 IT vendors ($651 million to 68 IT vendors from 2013/14 to 2018/19) that provided critical IT services to support its business operations. Any interruption to OLG's lines of business had the potential to reduce the province's revenue and impact OLG's gaming customers' experience.

The following were some of our significant findings:

- OLG needed to strengthen its oversight of IT vendors so that they delivered services and safeguarded customer information more effectively and in accordance with the performance expectations in their contracts.
- OLG did not thoroughly review IT vendors' performance upon contract renewal to assess whether

the vendor had met OLG's performance expectations under its previous contract.

- Although OLG conducted regular vulnerability assessments, OLG had not regularly performed security tests, such as penetration testing for its lottery and iGaming lines of business, to further identify potential vulnerabilities.
- Personal information of OLG customers was encrypted to prevent external access to it; however, seven OLG employees had access to the information in an unencrypted form, which increased the risk of customers' personal information being read for inappropriate purposes. In addition, we found that two casinos did not comply with OLG information security standards and did not encrypt OLG customer data within their IT systems.
- There were opportunities to strengthen cybersecurity practices in the IT systems used in casinos, lottery and iGaming. For example, although OLG had contracted with an external IT vendor to assess the technical controls behind the random number generator for its lottery system and evaluated the software formula to confirm that the system was able to generate suitable random numbers, we noted that OLG did not review the software source code for cybersecurity weaknesses using industry best practices.
- OLG had not developed and tested a comprehensive disaster recovery strategy for its entire IT system environment. Although there were disaster recovery strategies developed and tested for IT systems for each individual line of business, we noted that OLG did not have a comprehensive strategy that incorporated all IT systems cohesively, even after it had a significant event occur that should have triggered OLG to prepare one.
- OLG had initiated major IT projects across various lines of its business. OLG had implemented 33 IT projects within budget between 2013/14 and 2018/19; however, the remaining 11 had been over budget ($91 million sampled over a total of $232 million spent), with delays and cost overruns of over $10 million.

We made 14 recommendations, consisting of 23 action items, to address our audit findings.

The Ontario Lottery and Gaming Corporation committed that it would take action to address our recommendations.

Status of Actions Taken on Recommendations

We conducted our follow-up work between March 2021 and August 2021 for the Ontario Lottery and Gaming Corporation (OLG). We obtained written representation from OLG that effective November 22, 2021, it has provided us with a complete update of the status of the recommendations we made in the original audit two years ago.

OLG Not Always Thoroughly Measuring and Monitoring IT Vendor Performance, which Can Impact Customer Experience

Recommendation 1

To improve oversight of the quality of the services provided by IT vendors, we recommend that Ontario Lottery and Gaming Corporation establish appropriate performance indicators and targets to be incorporated in all service-level agreements, monitor performance against the targets and, where necessary, take the necessary action to correct any concerns.

Status: Fully implemented.

Details

In our 2019 audit, we found that OLG's oversight over its IT vendors could be improved. In order to enforce vendor accountability and ensure IT system service quality expectations are clearly understood and met, performance indicators—such as for service availability, system capacity and IT incident resolution time—should be included in vendor

contracts. We found that three of the 10 contracts for IT vendors that we reviewed did not have the necessary performance indicators within their service-level agreements. As such, OLG did not have a contractual mechanism for tracking vendor accountability in meeting service quality.

In our follow-up, we noted that in July 2020, OLG updated its current standard contract process by incorporating a new contract template (titled as "Support and Service level Agreement") to ensure that appropriate performance indicators and expectations or achievement rates, along with monitoring interval (i.e., monthly or quarterly), are set forth for IT services procured at OLG. In addition, OLG strengthened its procurement division to have skilled resources to improve oversight for IT procurement management, including the development of requests for proposals and negotiation of requirements and expectations of proposed vendors.

Recommendation 2

To improve oversight of IT vendors, we recommend that Ontario Lottery and Gaming Corporation review vendors' performance regularly in accordance with their service-level agreements and take appropriate action when targets are not met.

Status: Fully implemented.

Details

Our 2019 audit found that the vendors of three IT systems to casinos—Omnigo (facial recognition), NRT (cash handling), and Avatar (the prevention of money laundering)—were not effectively monitored by OLG in accordance with their service-level agreements. For example, according to the service-level agreements, monthly and quarterly performance meetings should be taking place between OLG managers and the IT vendors. We found that OLG had not been holding meetings with these vendors or obtaining performance reports to know whether service standards were met.

In our follow-up, we found that, in March 2020, OLG implemented an IT vendor classification framework and scorecards with performance targets to properly manage technology vendors. In addition, OLG performed a review of its third-party management process to provide a recommendation document so that it can further improve the overall framework for the enterprise-wide vendor management process. We further reviewed the IT vendor classification framework and performance scorecards in accordance with their service-level agreements, along with the sample selection, and noted that OLG established consistent criteria to classify IT vendors and review and follow up on vendors' performance for corrective actions. Refer to **Recommendation 3** and **Recommendation 4** for more details.

Recommendation 3

To enable the appropriate classification of IT vendors and enable them to be subject to the appropriate level of oversight, we recommend that Ontario Lottery and Gaming Corporation:

- *establish consistent criteria for classifying existing and new vendors when it initiates contracts with them, using the selection factors identified by industry best practices;*

  Status: Fully implemented.

Details

In our 2019 audit, we found that although OLG has three vendor categories (strategic, tactical or commodity) and guidelines associated with them, there was no consistent approach for determining a vendor's classification. We noted that the classification was subjective and based on OLG IT operations' perception of its vendors. For instance, according to the vendor categories and guidelines, every IT vendor with an annual contract value of $1 million or more is to be classified as strategic; however, we found that 13 of the 51 vendors classified as tactical (25%) were paid over $1 million each year in the past five years. As a result of being classified as tactical, these vendors were subject to less oversight—being reviewed quarterly instead of monthly.

In our follow-up, we found that in December 2019, OLG implemented a Technology Vendor Classification framework to properly classify and manage

technology vendors as per the significance of service they provide to OLG. Prior to implementing the Technology Vendor Classification framework, OLG analyzed and incorporated industry best practices into the framework, including the Gartner vendor segmentation model/toolkit and Institute of Internal Auditors' IPPF Guide. We also noted that the responsible vendor integration (or IT) managers conducted their assessment by category (i.e., financial risks, significance of their operations to OLG's reputation, size of their contracts and the type of services they provide to OLG operations) with associated scoring criteria to ensure a consistent review process.

- *review vendors' classifications at least annually and also when any significant changes to vendor operations occur.*

  Status: Fully implemented.

Details

Our 2019 audit found that OLG did not review vendors' classifications on a regular basis to ensure that IT vendors are subject to proper oversight based on their classifications.

In our follow-up, we found that the vendor integration managers reviewed the Technology Vendor Classification framework to identify any changes required to existing technology vendors or their lines of services to ensure vendor ratings are based on the evaluation criteria. OLG completed its first annual vendor classification review in December 2020. We noted that 43 out of 163 technology vendors (26%) had their classification revised from their classification as of December 2019 based on the review performed (i.e., strategic, tactical or commodity) during the annual review in December 2020.

Recommendation 4

To continually confirm the importance of IT vendors meeting their contractual performance commitments, we recommend that Ontario Lottery and Gaming Corporation track vendors' performance and collect the payments specified in the service-level agreements.

Status: Fully implemented.

Details

Our 2019 audit found that four of the 10 IT vendors we selected to review had a clause in their service-level agreements requiring them to pay a penalty to OLG if they did not provide IT services in accordance with their service-level agreements. We noted that two out of the four vendors in our sample missed their performance targets, but OLG did not enforce the penalty payment. When OLG does not enforce this requirement, its vendors may have less incentive to reach their performance targets.

In our follow-up, we found that OLG defined and incorporated the vendors' performance metrics (KPIs) into scorecards for regular monitoring and reporting on strategic vendors' performance. OLG also updated its existing procedures to enforce service credits or penalties for vendors where penalty clauses were included in their contracts. When performance targets are not achieved against the defined Service level Agreement (SLA) in the respective contract, the vendor is to provide service credits or penalties subject to the contract terms. In addition, OLG implemented the Technology Vendor Management (TVM) process and training program that outlined the vendor integration manager's roles and responsibilities to ensure consistent oversight over various technology vendors.

Recommendation 5

To have a reliable backup for its primary Internet provider to help assure continuity of its business operations, we recommend that Ontario Lottery and Gaming Corporation analyze the costs and benefits of acquiring a secondary Internet provider.

Status: Fully implemented.

Details

Our 2019 audit found that Rogers Communications is the sole provider of Internet network connectivity to all lottery retailers in Ontario and is OLG's primary Internet connectivity provider. In a scenario where Rogers is experiencing a province-wide outage, OLG does not have a backup Internet provider to support its day-to-day operations.

In our follow-up, we found that OLG performed an assessment to analyze the associated costs and benefits of acquiring a secondary Internet provider to improve continuity of its business operations and minimize the impact of network outages. We noted that OLG conducted a trend analysis for the last four years (2017 to 2020) relating to retailer network availability and the time to repair outages. From the OLG analysis, we noted that incidents at retail locations had been reduced to fewer than two times per retail location in 2020 and that the service-level agreement (SLA) targets for the network availability and time to repair outages at retail location were met in 2020. In addition, OLG analyzed the potential lottery revenue impacts due to outages for the same time period. In consideration of significant incremental costs for a secondary network provider, OLG concluded that the cost would exceed any potential benefits. In addition, OLG performed a benchmark study of other regional lottery corporations across Canada and learned that they did not use a secondary network provider for lottery retailers.

Recommendation 6

To improve oversight of IT vendors, we recommend that before extending or renewing an existing contract, Ontario Lottery and Gaming Corporation:

- *perform thorough vendor performance assessments on its current vendors;*
  Status: Fully implemented.

Details

In our 2019 audit, we found that OLG extended IT contracts for four out of the 10 IT vendors we reviewed, with cumulative payments ranging from $1.5 million to $23.2 million, without thoroughly evaluating the vendors' performance. Effective governance over IT procurement and contracts requires that the overseer assess vendor performance—using tools such as performance scorecards, service and product quality reports, issue and problem logs and risk ratings—prior to renewing key IT contracts. Such assessments provide assurance to organizations that the vendors successfully provided goods and services in accordance with the agreements.

In our follow-up, we found that OLG improved the IT vendor contract renewal process by revising the renewal management procedures along with roles and responsibilities for key stakeholders, ensuring vendor performance assessment was conducted regularly, and offering procurement training for key stakeholders such as contract owners, vendor integration managers and procurement specialists. Refer to **Recommendation 4** for more details. In addition, OLG has implemented a new feature related to renewal management activity in the contract management IT system (ContractHub) to allow Procurement to initiate renewal activities with contract owners, including evaluating active contracts and capturing vendor performance reviews from business units.

- *improve the existing procurement process by assessing whether a new tender for service is more appropriate than extending or renewing its contracts.*
  Status: Fully implemented.

Details

In our follow-up, we found that OLG improved the existing procurement process so that it now requires a business case (cost and benefit analysis) for evaluating whether a new tender for service is more appropriate than extending or renewing its existing contract. We reviewed a sample of an assessment conducted for the existing software that provides a service to OLG so that it can share files securely with external parties. As per the assessment performed by the OLG IT Solution Delivery team, we found that OLG's IT was advised to explore other options based on the solution assessment as part of its cost and benefit analysis. As a result, OLG IT decided to leverage the existing system which had the file-sharing capability instead of renewing the contract.

Recommendation 7

To strengthen oversight of IT vendors, we recommend that Ontario Lottery and Gaming Corporation (OLG):

- *clarify and communicate to OLG IT managers their roles and responsibilities for overseeing vendors' compliance with the contractual service commitments in their service-level agreements;*
  Status: Fully implemented.

Details

In our 2019 audit, we found that performance meetings were not taking place as required under the contracts. The 10 managers we interviewed told us that their roles and responsibilities are not well defined and they were not clear about their job requirements in this area. Clarifying their responsibilities is needed to ensure that they hold the performance meetings (by phone or in person) as required in vendors' contracts.

In our follow-up, we found that OLG implemented a Technology Vendor Management (TVM) process and training program that outlined the vendor integration manager's roles and responsibilities and provided guidelines for consistently implementing the TVM process. The TVM process includes detailed accountabilities for vendor managers such as managing technology contract obligations/SLAs, regularly monitoring vendor relationships and performance targets, and ensuring risk management (e.g., Threat Risk Assessments) in order to effectively manage vendor performance.

- *develop guidance for OLG managers on what constitutes effective monitoring of vendor performance.*
  Status: Fully implemented.

Details

Our 2019 audit found that information about vendors, such as past vendor contracts, vendor activities, meeting minutes and performance reports, is not stored in the central IT repository or readily available. As a result, we found that OLG managers did not have key information on past trends and activities relating to vendor performance.

In our follow-up, we found that OLG developed and implemented vendor management related training resources within the corporate training system and that all vendor integration managers are required to complete the training. We noted that OLG obtained an annual attestation from all 52 IT managers that they have completed the training as of June 1, 2021.

Security over Personal Information of OLG Customers and Employees Can Be Strengthened

Recommendation 8

In order for Ontario Lottery and Gaming Corporation (OLG) to more effectively protect itself from the risk of cyberattacks, safeguard personal information, and have continuity of services, we recommend that OLG regularly perform penetration testing of all critical IT systems.

Status: Fully implemented.

Details

We found in our 2019 audit that although OLG conducts regular vulnerability assessments, OLG had not regularly performed penetration testing to further identify cybersecurity vulnerabilities. Specifically, we noted that its iGaming website, PlayOLG.ca, had not been tested regularly since it was launched in January 2015. We noted that it was last tested in 2016 and 2017. In addition, OLG had not performed a penetration test of the OLG Lottery Mobile App, which was developed by an IT vendor and stores customers' personal information. A potential breach via the app increases the risk that customer data, including customers' names, addresses and telephone numbers, could be compromised.

Since our audit, we found that in June 2020, OLG established a security policy for system vulnerability penetration tests that outlines criteria, assessment scope and scheduling, technical reporting and analysis, and mitigation and re-testing in order to regularly test OLG's critical IT systems. We noted that OLG performed penetration tests of the iGaming website, PlayOLG.ca in August 2020 and in April 2021, and of

the OLG Lottery Mobile App in February 2020 and in April 2021.

Recommendation 9

So that personal information is safeguarded against breaches, we recommend that Ontario Lottery and Gaming Corporation:

- *encrypt all personal information and restrict access using industry best practices;*
  Status: Fully implemented.

Details

Our 2019 audit found that OLG collects the personal information of customers for business purposes and regulatory compliance. The information is stored in OLG databases and is encrypted to prevent attackers from accessing it. However, we found that, at the time of our audit, OLG had seven employees who had unrestricted access to databases that hold all OLG's customers' confidential information. This is not in line with best practices for security. Best practices would require a system privilege account (such as a Firecall ID) instead of these seven individual privileged accounts. A "Firecall ID" is a method established to provide temporary and monitored access to sensitive and secured information.

In our follow-up, we found that OLG's Data Protection Policy includes that sensitive information assets, including personal information, must be safeguarded from unintentional disclosure by applying encryption techniques which will safeguard the information as it is stored, transmitted, or in use. We noted that OLG encrypted all personal information stored in the in-scope systems as recommended in our 2019 audit and implemented security controls such as the user and network access control to monitor and log privileged database administrators' access to such information.

- *review and where needed update its definition and classification of personal information annually;*
  Status: Fully implemented.

Details

In our 2019 audit, we also found that OLG has an overly narrow definition of personal data, so the personal information collected at casinos that does not meet this narrow definition is not safeguarded to the same extent as the personal information that does meet the definition. For example, OLG uses IT systems at casinos to identify restricted players: the IT system captures their images in photographs and compares them to a database of restricted players. These photographs are converted to mathematical formulae that are not classified as personal information by OLG. However, the Information and Privacy Commissioner of Ontario advised us that these mathematical formulae describing a person's facial geometry should be considered personal information.

In our follow-up, we found that OLG implemented the Protection of Privacy Policy in April 2020. The policy outlines the definition and classification of personal information and reporting of privacy breaches and issues, as well as roles and responsibilities of key stakeholders at OLG. The Protection of Privacy Policy specifies that the definition of personal information is to be reviewed on an annual basis. We also noted that OLG issued a communication about the new policy to all OLG employees, focusing on employees' responsibilities to comply with the policy requirements for protecting personal information.

- *ensure that data is disposed of according to the requirements of the* Freedom of Information and Protection of Privacy Act.
  Status: Fully implemented.

Details

In our 2019 audit, we found that the personal information of OLG's customers is within the purview of the province's *Freedom of Information and Protection of Privacy Act* (Privacy Act). The Privacy Act requires that OLG must maintain a record of the types of personal data it disposes of and the date of disposal. However, we found that OLG's IT division does not maintain such a record for its disposal of the personal information of lottery players and casino customers.

In our follow-up, we found that OLG updated the archiving system so that it now keeps records of the types and dates of disposed personal data. OLG also provided training to the personnel who have the custody of personal data to educate them about their accountabilities, including the Privacy Act compliance requirements. We reviewed data deletion logs from January to February 2021 and noted that OLG had maintained records of the date, incident ID, type, who requested the deletion and reason for disposed personal data.

Recommendation 10

To be compliant with its own standards, we recommend that Ontario Lottery and Gaming Corporation (OLG):

- *review and update its information security standards to specify how casinos are to protect personal information—for example, with encryption of personal information;*
  Status: Little or no progress.

Details

In our 2019 audit, we found that casinos are contractually required to store OLG's customer information in accordance with OLG's information security standards. However, we found that the standards state only that the casinos must protect the information, but are silent on how that needs to be accomplished. When we visited two casinos, we found that neither casino encrypts OLG customer data within its IT systems.

At the time of our follow-up, we found that OLG has not taken sufficient measures to ensure that casino operators protect personal information by applying safeguards such as encryption. We were informed by OLG that due to the COVID-19 pandemic, Ontario casinos have been closed since March 2020. As a result, casinos have limited number of staff to support their operations, resulting in delays for implementing encryption of personal data. OLG will work with each casino operator to define a roadmap, by June 30, 2022, for achieving full compliance with encryption requirements for personal information.

- *ensure that all casinos deliver their established formal training programs for their staff to reduce the risk of successful cyberattacks.*
  Status: Little or no progress.

Details

In our 2019 audit, we found that a data breach occurred in November 2016, when Casino A was hit with a cyberattack during which customer and casino employee data was stolen. OLG and the Office of the Information and Privacy Commissioner of Ontario indicated that the incident was due to a phishing email sent to Casino A employees resulting in the theft of approximately 14,000 records, including financial reports, customer credit inquiries, collection and debt information, and payroll and other data. Following the Casino A incident, OLG strengthened existing provisions in the agreements with its casino operators to ensure that data breaches are addressed and reported to OLG in accordance with OLG's information security practices. However, OLG has not confirmed that casinos are providing guidance to their employees, on an ongoing basis, to prevent a similar incident from occurring. We also noted that two more phishing attacks have happened since then. These two incidents were similar to the Casino A incident, where employee awareness of these suspicious emails could have prevented the incident.

At the time of our follow-up, we noted that OLG has made little or no progress in ensuring that all casino operators deliver information security awareness training to their staff on an annual basis. This has been delayed due to the closure of Ontario casinos and limited number of casino personnel to support their operations during the COVID-19 pandemic. OLG has drafted the minimum guidelines for an information security awareness program to clarify and strengthen specific requirements for the casino operators. OLG will communicate the requirements to the casino operators by October 30, 2021, and plans to implement the recommendation by June 30, 2022.

Additional Steps Could Be Taken to Further Reduce Cybersecurity Risks for Lottery, Casino and iGaming Systems

Recommendation 11

To improve the security over the generation of lottery numbers and identify cybersecurity weaknesses in the iGaming and casino IT systems, we recommend that Ontario Lottery and Gaming Corporation review its software source code in accordance with industry best practices.

Status: In the process of being implemented by December 2021.

Details

In our 2019 audit, we noted that OLG's IT team does not review the software source code of the critical IT systems that are used for its lottery, iGaming and casino operations. Software source code consists of instructions written by a programmer that can be read by humans. Although the software source code from iGaming and casinos is reviewed by the vendor supporting these IT systems, OLG does not follow the industry best practice of identifying cybersecurity weaknesses by either performing an independent review of software source code or ensuring that vendors diligently perform such reviews.

In our follow-up, we found that OLG has updated the System Development Life Cycle (SDLC) process to designate source code reviews as mandatory. OLG is in the process of finalizing the software source code policy to define source code review requirements and by selecting a software tool to achieve the source code review requirements. OLG plans to finalize and implement the policy with the software analysis tool by December 31, 2021.

Comprehensive Disaster Recovery and Testing Strategy Needed

Recommendation 12

To manage risks to key information technology systems at Ontario Lottery and Gaming Corporation (OLG), we recommend that OLG:

- *establish a comprehensive disaster recovery plan to be approved and tested on an annual basis for its entire IT environment;*

  Status: Little or no progress.

Details

In our 2019 audit, we noted that OLG does not have a comprehensive disaster recovery plan that incorporates all IT systems cohesively. This became apparent when OLG experienced a major outage for almost six hours on October 29, 2018, resulting in key IT systems such as the lottery system and the gaming management system being unavailable. We found that a network switch at the Toronto data centre failed at 12:47 p.m., and services were not restored until almost six hours later, at 6:38 p.m. We noted that as of the time of our audit, OLG had yet to develop and test a comprehensive disaster recovery strategy that would allow OLG to recover operations within its set targets.

In our follow-up, we noted that OLG engaged a third-party vendor and conducted a review of strategic technology resilience to incorporate the recommendations in establishing a comprehensive disaster recovery plan. In April 2021, OLG developed the disaster recovery plan working group and plans to implement the disaster recovery plan by December 31, 2022.

- *review its information systems classification on a periodic basis for consistency across OLG and casino IT systems;*

  Status: Little or no progress.

Details

We found in our 2019 audit that OLG classifies its 186 systems according to how critical they are to its business operations. The classifications determine whether a disaster recovery test is required and, if so, how frequently tests should be done and how quickly OLG should be able to recover those systems. We noted that OLG has not reviewed the classifications for its systems to ensure the adequacy of their ability to meet their targeted recovery time is being tested.

In our follow-up, we found that OLG has made little or no progress on reviewing its information systems classification on a periodic basis for consistency across OLG and casino IT systems. OLG plans to implement this recommendation by December 31, 2021.

- *retest the disaster recovery plan for its IT systems following each failed disaster recovery test.*
  Status: Fully implemented.

Details

In our follow-up, we found that OLG implemented a process to keep track of disaster recovery plan tests for its IT systems in December 2020. This process also ensures that when a disaster recovery plan test fails, for example, not meeting the target recovery time in less than four hours or within 24 hours depending on how critical those IT systems are to OLG operations, corrective actions are taken to address the reasons for failure. Upon completion of the corrective actions, OLG schedules and performs retests of the failed disaster recovery plans to make sure they achieve passing results.

Certain IT Projects Have Experienced Delays in Implementation and About $10 Million in Cost Overruns

Recommendation 13

In order to successfully implement its digital strategy and avoid the risk of delays in implementation and cost overruns, we recommend that Ontario Lottery Gaming Corporation implement a project management framework that tracks, monitors and reports on all IT projects on a timely basis.

Status: Fully implemented.

Details

In our 2019 audit, we found that OLG has implemented 44 IT projects at a cost of $232 million across its various lines of business over the last five years, such as the introduction of the Internet gaming website PlayOLG.ca (iGaming) and the OLG Lottery Mobile App, and has upgraded key IT systems at casinos and charitable gaming sites (cGaming). OLG implemented 33 IT projects within budget. However, the remaining 11 projects, which accounted for almost half of all IT project expenses over the last five years ($91 million sampled over a total of $232 million spent), experienced delays and cost overruns of over $10 million. We noted that there were multiple factors that contributed to the delays and cost overruns, such as weaker project oversight and monitoring.

In our follow-up, we found that in January 2020, OLG implemented a new project control framework to strengthen oversight that tracks, monitors and reports on IT projects on a timely basis. We reviewed the sample IT project and corresponding supports. We noted that business case, project charter, project implementation plan, project change request and weekly status reports to manage project implementation, as well as post project review, were completed in line with the new project control framework. OLG has also provided project governance training to the Project Management Office staff and key Technology and Finance stakeholders so that they understand

the new project management framework and their responsibilities.

OLG Internal Risk and Audit Division Not Performing Independent Audits of All Casinos to Reduce IT Risk

Recommendation 14

To improve the effectiveness of oversight of IT operations at casinos, we recommend that Ontario Lottery and Gaming Corporation's (OLG's) Risk and Audit Division:

- *audit casino operators' performance of their IT responsibilities on a periodic basis to assess their compliance with contractual and regulatory requirements;*

  Status: In the process of being implemented by March 2023.

Details

We found in our 2019 audit that OLG's Internal Risk and Audit Division had not performed the independent IT audits at all casinos as allowed under the Agreements. The Risk and Audit Division performed only 15 IT audits for the 26 casinos, and these audits had a limited scope. This does not provide sufficient assurance of casinos' compliance with their IT responsibilities under the Agreements.

At the time of our follow-up, we found that OLG developed an Internal Audit Plan to provide assurance over Casino Operators' IT controls and to ensure full coverage of all casino operators as part of a three-year cycle from April 2020 to March 2023. The audit plan also includes IT audit scope such as user access control, security vulnerability management, data protection and user information security awareness programs.

We noted OLG Risk and Audit Division performed the IT audit that covered 11 casinos (39%, out of 28 casinos) in 2021.

- *formally review external audit reports to identify IT risks impacting OLG's business operations and to confirm that corrective action has been taken.*

  Status: Little or no progress.

Details

In our 2019 audit, we also found that where audits of casinos were performed by OLG's external auditors, OLG's Internal Risk and Audit Division did not review the audit reports to assess whether the audits identified system weaknesses and risks to IT operations impacting OLG. We reviewed these reports and noted that the audit reports identified weaknesses such as user access concerns and weak security controls for key systems.

Since our audit, OLG's Risk and Audit Division has made little progress in reviewing IT risks identified by casino operators' external auditors to assess the impact on OLG's operations and confirm that corrective actions have been taken. We noted that the external IT audit report performed by OLG's external auditors (KPMG) in the 2019/20 fiscal year was reviewed but the remediation plans were not completely implemented by casino operators. We also noted that OLG received six IT audit reports performed by casino operators' auditors in the 2020/21 fiscal year. Although OLG reviews and follows up the findings from the casino operators' IT audit reports, we noted that OLG did not perform a formal assessment to identify IT risks impacting OLG's business operations.

In addition, we noted that two casino operators (Hard Rock Ottawa and Caesars Entertainment) did not provide any IT audit reports in the 2020/21 fiscal year for OLG's formal review.