Chapter 3
Section
3.13

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

1.0 Summary

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 26 casinos currently operating in Ontario (casinos).

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 tests the design of OLG's games for the games' integrity and to ensure that players receive a fair payout.

OLG's website provides advice to its customers on its games and on issues around gambling. To fulfill its responsibility under the *Ontario Lottery Gaming Corporation Act, 1999*, "to promote responsible gambling," OLG administers the PlaySmart program, which lets players limit their exposure to gambling. Similarly, OLG sends out reminders to online players when they reach a certain limit in money wagered.

OLG contributed about 45% of the total $5.47 billion in non-tax revenue generated in 2018/19 by provincial government business enterprises, which also include 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 $651 million to 68 IT vendors that provide critical IT services to support its business operations. Any interruption to OLG's lines of business has the potential to reduce the province's revenue and impact OLG's gaming customers' experience. Outages and other incidents could negatively affect the experience of thousands of OLG customers—including purchasers of lottery tickets at any of Ontario's 10,000 lottery retailers, who expect the terminals and the OLG Lottery Mobile App to be working properly, scanning tickets accurately and displaying winning numbers and

coupons correctly—as well as casino customers and players of online games who want to be assured that the game they are playing is being run fairly.

We found that OLG needs to strengthen its oversight of IT vendors so that they deliver services and safeguard customer information more effectively and in accordance with the performance expectations in their contracts. OLG does not thoroughly review IT vendors' performance upon contract renewal to assess whether the vendor met OLG's performance expectations under its previous contract. As well, we found that casinos do not fully secure customers' personal information stored on their servers according to industry best practices.

There are opportunities to strengthen cybersecurity practices in the IT systems used in casinos, lottery and iGaming. For example, although OLG contracts with an external IT vendor to assess the technical controls behind the random number generator for its lottery system and evaluate the software formula to confirm that the system is able to generate suitable random numbers, we noted that OLG does not review the software source code for cybersecurity weaknesses using industry best practices. Although OLG conducts regular vulnerability assessments, OLG has not regularly performed security tests such as penetration testing for its lottery and iGaming lines of business to further identify potential vulnerabilities.

OLG has initiated major IT projects across its various lines of its business. OLG implemented 33 IT projects within budget; however, the remaining 11 were over budget, which account for almost half of all IT project expenses over the last five years ($91 million sampled over a total of $232 million spent), and had delays and cost overruns of over $10 million.

The following are some of our significant findings:

IT Vendor Performance

- **Critical IT performance indicators are not always incorporated in the service-level agreement with IT vendors.** Three out of the 10 service-level agreements we reviewed did not include key IT performance indicators. Depending on the service-level agreement, one or more critical performance indicators, such as system availability, service outages, incident resolution or response times, were not included, impacting (in various degrees) measurement of the customer experience, and, potentially, revenue and business operations.
- **Certain IT vendors are underperforming and not held accountable for meeting performance targets.** OLG does not consistently review the performance of all IT vendors against their service-level agreement and take remedial action where appropriate, such as imposing fines as per their service-level agreement. We found examples where IT vendors' performance was not reviewed by OLG. When we reviewed their performance, we noted that they did not meet their service-level-agreement performance targets, but remedial action was not taken by OLG because it had not reviewed their performance.

Cybersecurity, Encryption and Security Controls

- **OLG has not always kept up to date with its testing for security vulnerabilities on its IT systems.** Although OLG conducts regular vulnerability assessments, OLG has not regularly performed security tests such as penetration testing to further identify cybersecurity vulnerabilities. In November 2018, the OLG iGaming IT system was attacked by a hacker, making it unavailable for 16 hours and impacting customer experience. As well, three OLG casinos were subject to phishing email cyberattacks, a type of attack where sensitive information is compromised by the attacker. For example, at one casino, sensitive customer and employee data was stolen.

In the other two incidents, employee data was compromised.

- **Seven OLG staff have access to unencrypted confidential customer information.** Personal information of OLG customers is encrypted to prevent external access to it; however, seven OLG employees have access to the information in an unencrypted form, which increases the risk of customers' personal information being read for inappropriate purposes. In addition, we found that two casinos do not comply with OLG information security standards and do not encrypt OLG customer data within their IT systems.
- **Source code of critical IT systems is not assessed for cybersecurity risk.** We found that OLG does not follow industry best practices of reviewing the source code (the list of human-readable instructions that a programmer writes) for cybersecurity weaknesses within critical IT systems for its lottery, iGaming and casino operations.

Disaster Recovery

- **OLG has not developed and tested a comprehensive disaster recovery strategy for its entire IT system environment.** Although there are disaster recovery strategies developed and tested for IT systems for each individual line of business, we noted that OLG does not have a comprehensive strategy that incorporates all IT systems cohesively, even after it had a significant event occur that should have triggered OLG to prepare one. A significant outage of six hours in October 2018 affected key IT systems used for OLG's lottery. Because a comprehensive strategy was not in place, OLG was not able to promptly recover all its operations within OLG's targeted recovery times.

During the course of our audit, we noted that OLG began to act on some of our findings, such as improving its existing vendor management process, implementing an IT system to track contracts that are up for renewal and conducting better oversight of IT operations at the casino operators that manage day-to-day operations of casinos.

Overall Conclusion

Our audit concluded that the Ontario Lottery and Gaming Corporation (OLG) does not always exercise thorough oversight over IT vendors that provide services to OLG for its Internet gaming, charitable gaming and casino operations. This is especially significant because of how heavily OLG relies on these IT vendors. OLG's IT contracts do not always contain the necessary performance indicators needed to ensure operations are delivered efficiently. As a result, OLG cannot always hold vendors accountable through their contracts when they do not provide the level of contracted services it expects.

We also found that the personal information of OLG customers is not fully protected, because the information is not securely stored on OLG's servers and by certain casino operators. Although OLG conducts regular vulnerability assessments, OLG has not regularly performed security tests such as penetration testing for its lottery and iGaming lines of business to further identify potential vulnerabilities.

At the time of our audit, OLG had not performed a comprehensive disaster recovery exercise that incorporates all lines of business to assess whether it would be able to restore its business operations in the event of an actual disaster such as a power outage or a large-scale cyberattack.

Our audit also concluded that OLG had systems in place to ensure that all customers who played OLG's Internet games were the appropriate age. As well, based on sample testing of selected casinos, we noted that OLG has been reporting appropriately to the Financial Transactions and Reports Analysis Centre of Canada on a timely basis.

This report contains 14 recommendations, with 23 action items, to address our audit findings.

OVERALL OLG RESPONSE

The Ontario Lottery and Gaming Corporation (OLG) thanks the Auditor General and her team for this report on Technology Systems (IT) and Cybersecurity at OLG.

OLG strives for continuous improvement and is committed to secure delivery of operations that safeguards personal information, achieves value for money from external IT vendors and minimizes business interruption that may impact revenue to the province.

To help support our digital evolution, OLG has selected service providers through open, public procurements to launch an integrated player platform, including a new gaming website and mobile applications; and is replacing and upgrading our retail point-of-sale system, including a state-of-the-art network and new lottery terminals.

As part of this important work, OLG is strengthening its management of vendor performance by, among other things, centralizing and strengthening the management of key IT vendors to ensure consistency and effective performance monitoring. We are making continuous investments in the protection of personal information and are implementing further measures to strengthen security controls and practices. We are improving project management governance and performance by launching a new project control framework to strengthen oversight through rigorous standards and processes.

As OLG evolves, we are maintaining our commitment to strong governance and are ensuring that effective measures are in place to deliver value for money to the province. OLG will continue to work with service providers, vendors and the Alcohol and Gaming Commission of Ontario to implement the Auditor General's recommendations.

2.0 Background

2.1 Overview of Ontario Lottery and Gaming Corporation

Ontario Lottery and Gaming Corporation (OLG) is a Crown corporation and is the most significant source of non-tax revenue for Ontario. OLG accounted for 45% of the total $5.47 billion in non-tax revenue generated in 2018/19 by government business enterprises such as the Liquor Control Board of Ontario, Ontario Power Generation Incorporated, Hydro One Limited, the Ontario Cannabis Retail Corporation and OLG itself (see **Figure 1**).

In 2018/19, OLG business operations generated $8.3 billion in revenue and $2.47 billion in net profit to the province. **Figure 2** provides OLG's revenue and net profit from its four lines of business for the last five fiscal years.

Ontario established the Ontario Lottery Corporation (OLC) in 1975, approximately six years after the federal *Criminal Code* was amended to authorize provincial lotteries. Under

Figure 1: Government Business Enterprises' Contribution to Non-Tax Revenue for Ontario, 2018/19

Source of Data: Public Accounts of Ontario, *Volume 1, 2018–2019*

Government Business Enterprises	Contribution ($ million)	Contribution (%)
Ontario Lottery and Gaming Corporation	2,464	45
Liquor Control Board of Ontario	2,276	42
Ontario Power Generation Inc.	837	15
Ontario Cannabis Retail Corporation	(42)	(1)
Hydro One Limited	(65)	(1)
Total contribution to the province	**5,470**	**100**

Figure 2: Ontario Lottery and Gaming Corporation (OLG) Revenue and Net Profit to Province, 2014/15–2018/19 ($ million)

Source of data: Consolidated Financial Statements in the OLG *2018/19 Annual Report*

OLG Lines of Business	2014/15	2015/16	2016/17	2017/18*	2018/19*
Lottery	3,269	3,786	3,681	3,780	4,167
cGaming (Charitable gaming)	115	166	153	172	183
Casinos (Land-based gaming)	3,252	3,444	3,583	3,796	3,857
iGaming (Internet gaming)	8	49	58	73	92
Total revenue	**6,644**	**7,445**	**7,475**	**7,821**	**8,299**
Net profit to the province	**1,999**	**2,231**	**2,361**	**2,487**	**2,471**

* Starting in the 2018/19 fiscal year, OLG adopted International Financing Reporting Standards (IFRS) 15 and IFRS 9. Comparative figures in 2017/18 have been reclassified, where necessary.

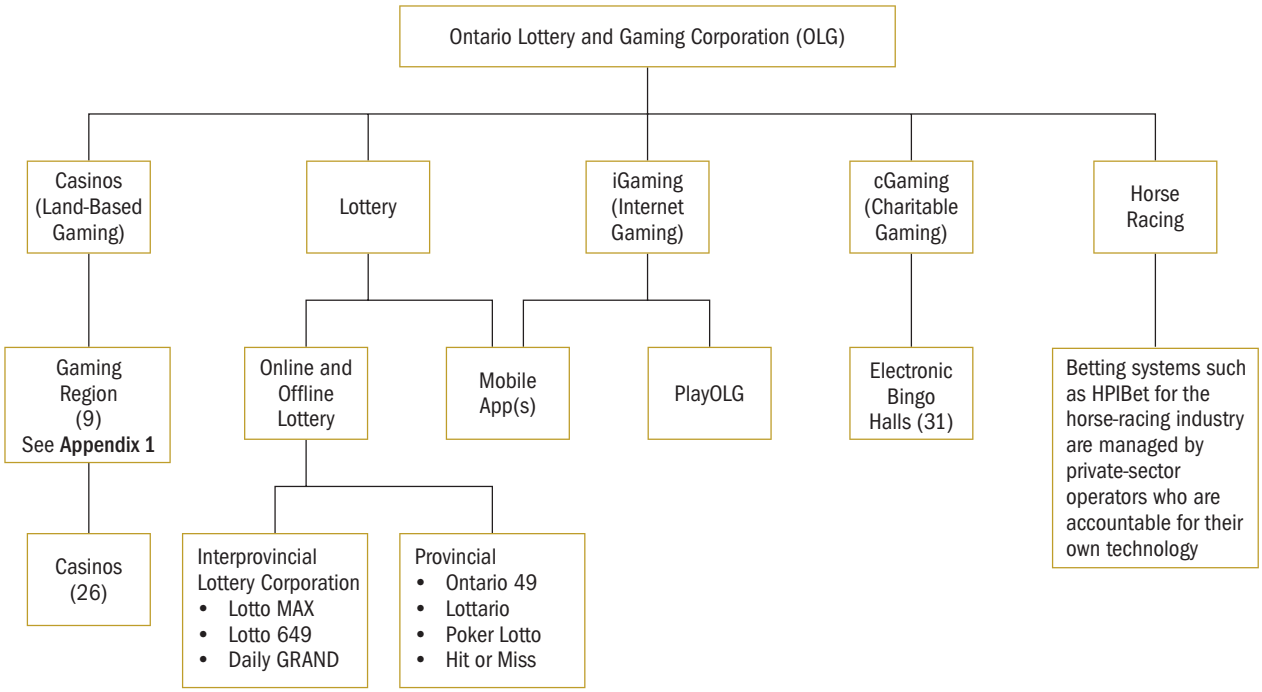
the government's Northern Ontario Relocation Program, the lottery corporation moved its head office to Sault Ste. Marie in 1991. In 1993, OLC approved a framework for licensing charities to raise funds through gaming. The government established the Ontario Casino Corporation (OCC) in 1994 and opened its first casino, in Windsor, that same year. The government ran its first electronic bingo game in 1997. The following year, the Alcohol and Gaming Commission of Ontario was created, and in 2000 the province merged the two corporations, OLC and OCC, into OLG. Today, OLG operates one data centre in Sault Ste. Marie and one in Toronto.

2.2 Lines of Business

OLG has four lines of business that are distinct revenue-generating divisions offering different products and services. These are land-based gaming (casinos), lottery, Internet gaming (iGaming) and charitable gaming (cGaming). OLG also has responsibility for funding the horse-racing industry on behalf of the province (see **Figure 3**).

- **Land-based gaming (casinos):** There are 26 "gaming sites"—we refer to them in this report as casinos—across the province (see **Appendix 1**), such as Casino Windsor, Casino Rama and Casino Niagara. These include slots and casinos operated by casino operators such as Caesars Entertainment, Windsor Limited, Gateway Casinos and Entertainment Limited. Casino operators report revenue to OLG through their IT gaming management systems, which are connected to the OLG central IT gaming management system. OLG validates revenue data and reviews audited financial statements provided by casino operators to ensure that revenues are complete and accurate.
- **Lottery:** Lottery games refer to national and regional lottery products where tickets are generated on a lottery terminal. Lottery products are sold by approximately 10,000 retailers across the province and through the OLG website PlayOLG.ca.
- **Internet gaming (iGaming):** PlayOLG.ca is the website-based gaming platform and was launched in January 2015. The website offers slots and electronic table games as well as sales of select lottery games—for example, Lotto MAX, Lotto 6/49 and Encore.
- **Charitable gaming (cGaming):** OLG operates electronic charitable games such as lottery, bingo and raffle tickets at registered charities and non-profit and service clubs across Ontario to support their communities. There are 31 charitable bingo and gaming centres that work with OLG to offer paper and electronic games.

Figure 3: Ontario Lottery and Gaming Corporation Key Lines of Business
Prepared by the Office of the Auditor General of Ontario



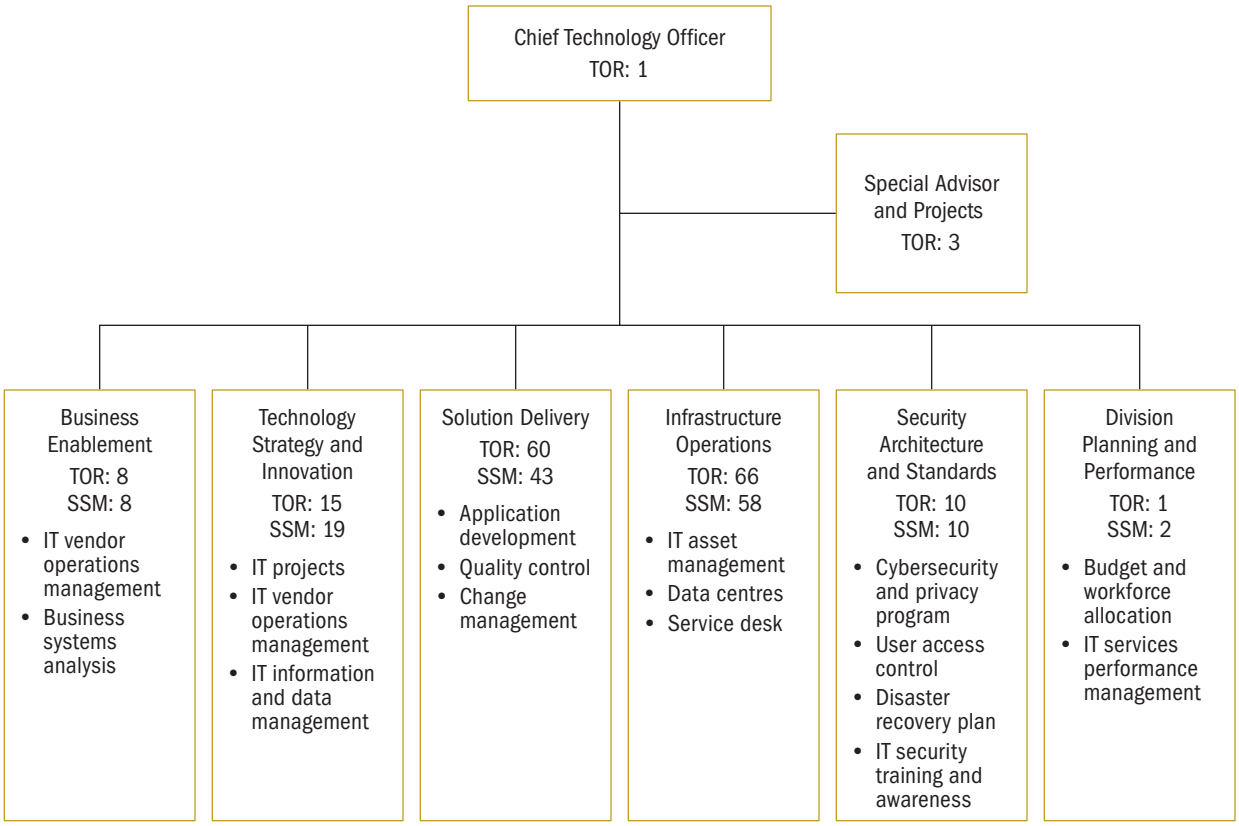
- **Horse racing:** OLG administers the Horse Racing Partnership Funding Program on behalf of the Ontario government and provides funding to the horse-racing industry in accordance with the administration agreement between the Minister of Finance and OLG. The OLG Technology Division has no resourcing involvement, support or oversight for technology systems in the horse-racing industry. Industry betting systems such as HPIBet are managed by private-sector operators who are accountable for their own technology. OLG informed us that its Horse Racing Division has approximately 12 staff who support the transfer payments to the industry. The horse-racing industry is not part of this audit, but it is the topic of **Section 3.12** in this chapter.

2.3 Information Technology Systems

The Corporate Services division of OLG, including Information Technology, Finance, Human Resources, Governance Legal and Compliance, and Audit Services, provides support services to all lines of business. OLG signs contract agreements with casino operators delegating to the operators the management of the day-to-day IT operations of casinos. It also signs contracts with IT vendors delegating IT management of the day-to-day IT operations of iGaming and cGaming to the IT vendors. However, OLG is still directly responsible for the day-to-day management of lottery IT operations.

IT systems are a critical component of OLG's core operations of casinos, lottery, iGaming and cGaming. OLG develops and maintains key IT systems for its lottery line of business. In addition, OLG has licensing agreements with IT software and hardware vendors to use their services for their other three lines of business. For example, OLG has contracted with the IT vendor Internet Gaming Technology (IGT) to develop and maintain

Figure 4: IT Division's Staff Allocation at Toronto (TOR) and Sault Ste. Marie (SSM), 2018
Source of data: Ontario Lottery and Gaming Corporation



its iGaming website. The IT system is hosted by the vendor. Also, IT systems such as Bally Gaming Management Systems and Casinolink, used at casinos for day-to-day business operations and to collect customer information, are owned by IT Vendors and operated by OLG through licensing agreements. The IT systems from IT vendors used for cGaming are licensed by OLG. See **Appendix 2** for a list of key IT systems.

2.4 IT Division

The IT division within OLG is responsible for the operation and maintenance of OLG's information systems and technology infrastructure for lottery operations. It is also responsible for exercising operational oversight over IT vendors' services delivered for iGaming and cGaming, as well as for oversight of casino operators' IT services at casinos.

The division spent $99 million on operating costs in 2017/18 (the most recent year that data was available). Operating costs have remained consistent, at 2% of OLG's total expenses, over the last five fiscal years.

The OLG IT division comprises six departments that help operate all four lines of business, with 304 full-time equivalent positions (costing $36.5 million) as of 2018, with 45% in Sault Ste. Marie and 55% in Toronto. **Figure 4** illustrates the IT division organization chart along with the budgeted IT staff allocation in the two offices.

The OLG Information and Technology Committee meets monthly to review IT projects, such as upgrading lottery terminals, and developing IT strategy to address risks and emerging trends.

2.5 Current Technology Projects

OLG is implementing a digital strategy that will let customers buy lottery tickets and play casino games through the OLG Lottery Mobile App. As part of this strategy, OLG will also offer more casino games on its Internet gaming website PlayOLG.ca. In addition, OLG is upgrading its existing lottery terminals at over 10,000 retail locations. OLG has spent a total of $232 million over the last five fiscal years for technology projects.

2.6 OLG Call Centre

The OLG call centre in Sault Ste. Marie offers customers and lottery retailers a 24/7 helpline. It is the first point of contact and supports all lines of OLG businesses: lottery, casinos, charitable gaming and online gaming. As of March 2019, the call centre had approximately 150 staff.

2.7 Cybersecurity

Cybersecurity is a critical measure to protect OLG from cyberattacks, privacy breaches, reputational damage, and the destruction of critical information and infrastructure, as well as from the negative financial impact that any of these could cause.

OLG has Information Security standards for its casinos that require them to protect the personal information of customers and staff. There has been a global increase in cyberattacks in the casino and lottery industry, such as the cyberattack in March 2016 against the River Cree Resort and Casino and in June 2016 against the Cowboys Casino, both located in Alberta. The National Lottery of the United Kingdom was hacked in November 2016 and September 2017, and twice more in March 2018.

We found that in the past five years, there have been thousands of unsuccessful cyberattack attempts at OLG. Examples of cybersecurity breaches at OLG are discussed in **Section 4.2**.

2.8 IT Procurement

OLG procurement is governed by external and internal policies and procedures. External policies and procedures include provincial legislation and directives, trade agreements and gaming regulations. Internally, OLG policies include financial approvals, a code of business conduct and a conflict-of-interest policy.

OLG uses the following procurement methods:

- an open competitive process involving the issuance of public procurement documents, such as requests for information, requests for prequalification and requests for proposal, using an electronic tendering system;
- an invitational process involving requests for a minimum of three qualified suppliers to submit a written proposal in response to OLG's requirements; and
- non-competitive procurement, which must be supported by a written business case that supports using a single or sole source and be approved by the appropriate authority:
  - single source selects one specific supplier even though several are capable of delivering the same goods or services; and
  - sole source selects a specific supplier based on the assessment that no other supplier is able to provide the required goods or services.

The Procurement Group within OLG is responsible for managing competitive evaluations to ensure IT procurement is performed consistently and in accordance with the evaluation criteria, ratings and methodology set out in the procurement documents that are issued to potential vendors by OLG. The documents identify the scope of work, evaluation criteria, terms of contracts and technology/solution specifications.

2.9 Responsible Gambling

Statutory requirements for OLG to "promote responsible gambling" were introduced in the

Ontario Lottery Gaming Corporation Act, 1999. OLG works with casinos to meet these standards and deliver the responsible-gaming program. OLG has a voluntary self-exclusion program, PlaySmart, that allows players to take a break from gambling at slots and casinos and on the Internet when they feel that gambling is no longer in their best interest. As of April 2019, 23,000 registered players were on the self-exclusion list across Ontario. At casinos, the program works through facial recognition technology, with the customer signing a contract with OLG. For Internet gaming, players have the option to set limits on how much money they spend. OLG also has controls such as disclaimers and reminders that it sends out when online players reach a certain limit in money wagered. OLG received the World Lottery Association's 2018 Best Overall Responsible Gambling Program award in recognition of its PlaySmart program.

Casinos also maintain a list of prohibited and excluded individuals, who are restricted from entering casinos due to various reasons, such as court orders, age limit (under 19 years) and improper dress.

2.10 Preventing Money Laundering at Casinos

Money laundering is the process used to hide the source of money or assets derived from criminal activity. Canadian casinos for many years have been used as "laundromats" for the proceeds of organized crime. Discovery of money laundering is difficult when the IT systems used to identify and report money laundering are ineffective and suspicious transaction reports are not reviewed regularly.

Casinos in Canada must fulfill specific obligations under federal regulations to help combat money laundering and terrorist financing. Although in Ontario casino operators are responsible for running casinos' daily operations, OLG is still responsible for the oversight of casinos and for ensuring compliance with federal regulations. For example, OLG is required to report to the Financial Transactions and Reports Analysis Centre of Canada (FinTRAC) any large cash transactions and other suspicious transactions. OLG has an Anti-Money Laundering Compliance Program whose purpose is to have all casinos in Ontario adhere to federal and provincial regulatory requirements.

2.11 Interprovincial Lottery Corporation

The Interprovincial Lottery Corporation (ILC) consists of five Canadian provincial lottery corporations, including OLG. The other members are British Columbia Lottery Corporation, Western Canada Lottery Corporation, Loto-Québec and Atlantic Lottery Corporation. ILC administers lotteries that are sold across Canada such as Lotto Max, Lotto 6/49 and Daily Grand. The provinces are paid revenue from the Canada-wide lotteries based on the proportion of ticket sales in their jurisdictions. OLG and the other four provincial lottery corporations oversee lotteries sold only within their provinces, like Lottario, where revenue remains within their jurisdictions.

2.12 Fairness of Gaming

The Alcohol and Gaming Commission of Ontario (Commission) ensures the integrity, security and fairness of gaming systems such as slots, electronic bingo machines and PlayOLG.ca games. As part of this, the Commission is responsible for the technical assessment and testing of all electronic gaming hardware and software and the associated equipment.

The Commission decides on the odds and payback percentages of OLG games, and OLG provides this information on its website. For example, the payback percentage of slot machines at casinos is a minimum 85%. The OLG website explains this as follows: "the payback percentage is representative of the machine's entire lifecycle, which can be many millions of spins. Thus, it does not mean that a player can expect to win back $85 if $100 was

gambled on that individual session." Such information is meant to inform customers openly and fairly of the game's risks and opportunities.

3.0 Audit Objective and Scope

Our audit objective was to assess whether Ontario Lottery and Gaming Corporation (OLG) has IT systems and processes in place for the:

- secure delivery of operations (including lottery operations) in an economic and efficient manner and in accordance with legislative, regulatory and contractual requirements;
- effective oversight of IT vendors who provide services to OLG for its Internet gaming, lottery, charitable gaming and casinos; and
- timely investigation and handling of cybersecurity incidents and fraudulent activities, such as money laundering and potential misuse of gaming systems.

In planning for our work, we identified the audit criteria we would use to address our audit objective (see **Appendix 3**). These criteria were established based on a review of applicable legislation, policies and procedures, internal and external studies, and best practices. Senior management at OLG reviewed and agreed with the suitability of our audit objective and related criteria.

We conducted our audit between January 2019 and September 2019. We obtained written representation from management that, effective November 18, 2019, they had provided us with all the information they were aware of that could significantly affect the findings or the conclusion of this report.

We conducted audit work primarily at OLG's Toronto and Sault Ste. Marie offices, which are responsible for the operation and maintenance of OLG's information systems and technology infrastructure, and for managing external technology vendors.

We also interviewed senior and front-line staff and reviewed documents. We were given a demonstration of lottery terminal machines used by retailers and the new lottery terminals that will be deployed in 2020. In Sault Ste. Marie and Toronto, we visited 20 retailers at gas stations, Gateway newsstands, casinos, convenience stores, shopping malls, cafés, grocery stores, drug marts and laundry services where OLG lottery terminals are deployed. We interviewed retailers regarding inventory count, IT-related incidents and training related to the use of terminals. We visited OLG's data centres in Toronto and Sault Ste. Marie to assess environmental and physical security controls. Environmental controls, which regulate such things as moisture, temperature and dust, protect IT equipment from damage and allow it to function optimally; physical security controls protect against risks such as tampering and theft. We were also given a demonstration of the IT asset disposal process at the Toronto office.

In addition, we met with staff at two casinos to review IT controls related to the prevention of money laundering, the collection and use of OLG's customer data, and the reporting of suspicious transactions to OLG and to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

We assessed IT systems and cybersecurity operations at OLG and reviewed governance oversight by OLG over its IT vendors and casino operators. We also assessed procurement practices at OLG and the protection and life-cycle management of critical IT assets and cybersecurity functions. We further reviewed whether casino operators and IT vendors deliver IT services to OLG as per service-level agreements.

In addition, we examined key IT projects implemented over the last five years that were in progress, as well as some projects that were planned as part of OLG's digital strategy. We reviewed project management (such as defined project requirements), the use of standard and consistent project

Figure 5: Assessment of IT Vendor Key Performance Indicators, January 2014–February 2019
Prepared by the Office of the Auditor General of Ontario

	Line of Ontario Lottery and Gaming Corporation (OLG) Business	Payments ($ million)	Vendor Classification	Performance Indicators in Contract	Performance Indicators Measured by OLG	Payment Clause in Contract	Payment Imposed (Poor Performance)
Section Reference				4.1.1	4.1.2	4.1.4	4.1.4
Vendor							
Avatar	Casino	0.9	Strategic	Yes	No	No	n/a
Bally	Casino	57.1	Strategic	No	Yes*	No	n/a
IGT Legacy (Casinolink/EZ Pay)	Casino	71.4	Strategic	No	Yes*	No	n/a
NRT	Casino	10.7	Tactical	Yes	No	No	n/a
Omnigo (iView)	Casino	3.0	Strategic	Yes	No	No	n/a
NCR Corporation	Lottery	34.2	Strategic	Yes	Yes	Yes	Yes
Plastic Mobile Inc.	Lottery	9.4	Tactical	No	n/a	No	n/a
Rogers Communications	Lottery	58.3	Strategic	Yes	Yes	Yes	No
Canadian Bank Note	Charitable Gaming	56.0	Strategic	Yes	Yes	Yes	No
IGT I-Gaming	I-Gaming	51.8	Strategic	Yes	Yes	Yes	Yes

* Performance indicators such as service availability are not established in the contract but are reviewed by OLG.

management frameworks, potential delays and under/over estimation of project costs.

We sampled 10 vendors (see **Figure 5**) from OLG's 68 IT vendors to examine whether performance metrics and IT services were delivered in line with the requirements included in their service-level agreements. The total amount spent on these 10 vendors from January 2014 to February 2019 was $353 million and accounts for over half of the IT expenses that provide critical IT services. These vendors were selected based on the payments they received, the different lines of business they served and the relevance of their operations to OLG's total revenues.

Based on the sample of OLG Internet customers we tested, we found that all customers who played OLG's Internet games were the appropriate age. We also tested names of lottery winners against names of OLG employees and found that, in accordance with OLG's policy, no employees had played the lottery and won a prize. We noted that there currently is an investigation to identify how suspects may have laundered money through the OLG casinos; however, based on sample testing of selected casinos, we noted that OLG has been reporting appropriately to FINTRAC on a timely basis.

4.0 Detailed Audit Observations

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

We found that Ontario Lottery and Gaming Corporation's (OLG's) oversight over its IT vendors can be improved. For example, OLG did not always

incorporate critical IT performance indicators into its service-level agreements with IT vendors, and where indicator targets were incorporated, IT vendors were not held accountable for meeting the related performance targets. The end result can be poor customer experience whenever casino gaming machines jammed, tickets and prizes were not processed, and system outages led to games and services not being available and casino operations being disrupted. See **Appendix 4** for information about the frequency of outages affecting key IT systems between January 2015 and May 2019.

4.1.1 Not All IT Vendor Contracts Contain Performance Indicators and Targets

Alcohol and Gaming Commission of Ontario standards, as well as industry best practices, advise that vendor contracts should include performance indicators that define the minimum performance targets for IT services and how the targets will be measured. 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 (see **Figure 5**). As such, OLG does not have a contractual mechanism for tracking vendor accountability in meeting service quality, as follows:

Plastic Mobile Inc. (line of business: lottery)

We found that performance indicators for service availability and capacity were not included in the contract for Plastic Mobile Inc. "Capacity" means meeting mobile users' peak volume (for example, during the peak day of Friday). Plastic Mobile Inc. is responsible for developing, testing, maintaining and hosting the OLG Lottery Mobile App for iOS (Apple) and Android, the operating system for Samsung, Motorola and other mobile models. The OLG Lottery Mobile App is used primarily for ticket scanning, jackpot information, displaying winning numbers and coupons. OLG paid Plastic Mobile over $9.4 million in the last five years. The contract was signed in January 2014 and has been amended three times since then; however, performance indicators for service availability and capacity have never been incorporated into the service-level agreement. The Alcohol and Gaming Commission of Ontario guidelines state that these performance indicators are minimum standard requirements to be incorporated in all service-level agreements.

We found that there were approximately 290 incidents impacting customer experience in the last five years pertaining to the OLG Lottery Mobile App ticket checker not being able to scan lottery tickets, and giving incorrect information regarding the displayed next jackpot draw date. We found there was no targeted turnaround time for resolving the IT issues; the time taken varied significantly, from one hour to 34 days. The average time taken was almost five days.

We noted that there is no requirement in the service-level agreement for Plastic Mobile Inc. to monitor its Lottery Mobile App's performance, and as a result, OLG is made aware of the app's outages and performance issues only when customers call the OLG call centre to complain.

IGT Casinolink and EZ Pay (line of business: casinos)

OLG paid IGT over $71.4 million in the last five years for the development and operational maintenance of the IT system used to connect games at casinos. The IT system is hosted by OLG, and IT support is provided by the vendor in accordance with the service-level agreement.

We found that the service-level agreement did not include a performance indicator for IT incident resolution time. We noted that approximately 3,000 IT incidents related to these IT systems

were recorded in OLG's call centre in the last five years. OLG assessed approximately 300 of these incidents as critical incidents that resulted in casino games not being available to customers, ultimately impacting their gaming experience and potentially impacting the casinos' revenue. Most of these incidents occurred during Fridays and Saturdays, which are generally peak days at casinos. The time to resolve the IT issues varied from one hour to 95 days; the average time was more than two days.

Bally Gaming Management System (GMS) (line of business: casinos)

We found that the service-level agreement with Bally did not include a performance indicator for IT incident resolution time. We noted that this system, which is used to collect casino gaming and customer information, had prolonged issue resolution times for recorded incidents relating to transferring customer and casino operational data from the casinos to OLG. We found that the Bally GMS had approximately 3,000 incidents in the last five years and that the vendor took as long as 600 days and an average of 26 days to resolve them. Among these incidents were business interruptions that primarily affected casino operations (not casino customers).

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.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) agrees with this recommendation and will establish enhanced vendor performance management oversight to ensure greater quality and accountability. As a result of the audit, OLG has strengthened standard contract templates to ensure appropriate metrics are defined. OLG is also developing new IT category management oversight within IT procurements to enhance the development of requests for proposals and improve the articulation of requirements and expectations of proposed vendors. OLG has reviewed and strengthened its vendor management process and additional resources to apply appropriate oversight to the performance of its vendors.

4.1.2 Achievement of Performance Targets Not Always Monitored by OLG

The vendors of three IT systems to casinos—Omnigo (facial recognition), NRT (cash handling), and Avatar (the prevention of money laundering)—are 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 has not been holding meetings with these vendors or obtaining performance reports to know whether service standards were met. As noted in **Section 4.1.6**, many OLG IT managers we interviewed told us that they were not clear about their job requirements for measuring vendors' compliance with their service-level agreements.

Omnigo Software (line of business: casinos)

Omnigo Software is a facial recognition and self-exclusion IT system used by OLG to detect and remove self-excluded customers from Ontario casinos (see **Section 2.9**). Omnigo's IT system is hosted by OLG, and support is provided by Omnigo as per the service-level agreement. The agreement's target for incident response ranges from 30 minutes to 48 hours, depending on the incident type, and incident resolution ranges from two hours

for critical incidents to five business days for non-critical incidents. We noted that Omnigo's performance in this regard was not reviewed by OLG.

We found that approximately 1,500 incidents have occurred in the last five years where the facial recognition IT system was not performing optimally across all casinos in Ontario. Over 300 of these were assessed as critical incidents by OLG. The most frequent incidents were facial detection errors, such as flagging the wrong customer for exclusion or failing to flag self-excluded customers, and delays in the security surveillance team receiving facial recognition alerts. We found that the average time to resolve these critical incidents was over four days instead of two hours.

NRT Technology Corporation (line of business: casinos)

NRT provides the cash handling system for automated jackpot dispensing machines and customer ticket redemption kiosks at casino sites. According to its service-level agreement, NRT is required to respond to IT incidents and resolve them within four hours. During quarterly performance meetings, OLG is required to review the performance relating to NRT's response to and resolution of IT incidents; however, we noted that OLG has not conducted a performance review since the contract was established in 2008. We found that casinos had experienced approximately 2,900 incidents in the past five years. These incidents included bills jamming inside kiosks at casinos and the NRT system not processing ticket vouchers and jackpot prizes for cash disbursement, impacting the overall customer experience. The resolution time for such incidents ranged from a few hours up to seven days.

Avatar Software Creations Inc. (line of business: casinos)

The Avatar IT system is used by OLG and casinos for reporting on money laundering to the federal regulator. According to its service-level agreement, Avatar is required to respond to and resolve incidents within four hours and provide service-level summary reports for performance review during quarterly meetings. However, we noted that OLG does not have performance meetings or receive the required service-level reports from Avatar. In addition, we found approximately 680 incidents taking up to 23 days to be resolved by Avatar. Such delays affect casinos' ability to promptly and accurately report transactions to OLG.

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.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) recognizes the importance of monitoring the performance of our IT vendors to maximize value for money. As a result of the audit, OLG has launched a comprehensive, enterprise review of its third-party management process and has established a revised management governance framework. This will result in more rigorous vendor reviews that assess performance against contracted standards and targets. In addition, OLG is improving its vendor classification, scorecards and management of service-level agreements.

4.1.3 Incorrect IT Vendor Classification Impacts OLG's Oversight

For its oversight purposes, OLG classifies IT vendors as strategic, tactical or commodity vendors, based on financial risk, significance of their operations to OLG's reputation, size of their contracts and the type of services they provide to OLG operations:

Figure 6: Categorization and Risk Level for Ontario Lottery and Gaming Corporation (OLG) Vendors
Source of data: Ontario Lottery and Gaming Corporation

Vendor Category	# of Vendors	Approximate Cumulative Annual Contract Values	Performance Meeting Frequency	Risk Level and Impact to OLG upon Supplier Failure
Strategic	17	>$1 million	Monthly	High
Tactical	51	$100,000–$1 million	Quarterly	Medium to high
Commodity	180	<$100,000	Not required	Low to medium

- **Strategic vendors** are subject to a higher level of oversight by OLG via monthly meetings where their performance is reviewed.
- **Tactical vendors** have quarterly performance meetings with OLG.
- **Commodity vendors** are not required to be reviewed for performance.

See **Figure 6** for further OLG guidelines regarding the three categories.

We found that although OLG has these three vendor categories 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, 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 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.

According to IT industry best practices, such as those put forth in the Control Objectives for Information and Related Technology and by the Institute of Internal Auditors, organizations should have a standard approach for classifying IT vendors. IT vendors should be classified based on factors such as financial impact, type of information residing with the vendor, cost, operational impact, third-party reliance, risk of fraud, public reputation and customer satisfaction.

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

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) agrees with the recommendation and understands the importance of having a standard approach for classifying IT vendors. As a result of the audit, OLG has redeveloped its IT classification methodology to align with industry best practices and has applied this against its current list of vendors. OLG will adopt a more rigorous vendor-and-performance-standards-review process, including annual classification reviews.

4.1.4 IT Vendors Not Held Accountable when They Miss Performance Targets

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 (see **Figure 5**). When OLG does not enforce this requirement, its vendors may have less incentive to reach their performance targets.

Rogers Communications is one of OLG's most critical IT vendors because it is the sole vendor responsible for providing Internet network services to all 10,000 lottery retailers in Ontario. If OLG does not monitor whether Rogers resolves incidents in a timely manner, customer experience may be impacted. If Rogers' network is unavailable, customers are not able to buy tickets, and ticket-holders and retailers are not able to check for winning tickets.

OLG uses a "credit system" with Rogers in which OLG charges Rogers a specified sum when service requirements, such as not meeting network availability and incident response-time targets, are not met. We found that OLG does not review Rogers' performance reports to ensure that the correct charges are being applied and that the reports are correct.

Specifically:

- As shown in **Figure 7**, OLG's contract with Rogers identifies seven categories of services for which OLG can charge Rogers for not meeting service-level requirements. We found that no payments had been made to OLG for three of the seven service categories when performance targets were not met. We identified over 90 instances in the past five years where IT service performance did not meet contract obligations.
- We cross-checked Rogers' performance reports against OLG 's incident-tracking tool and found that certain incidents that had been tracked by OLG were not noted in the performance reports. For instance, according to Rogers' performance reports, Rogers met service-level requirements for

Figure 7: Service-Level Agreement (SLA) Categories and Results for Rogers Communications

Prepared by the Office of the Auditor General of Ontario

Categories	SLA Target	Penalty if Performance is Lower than SLA Target	Penalty Imposed	# of Instances[1] Penalty Not Imposed If Applicable
1. Core network availability	99.99%	1%–25% of monthly connection charges for all sites (depending on service level score)	Yes	n/a
2. Site (retailer) network availability	99.90%	1%–20% of monthly connection charges for all sites whether cable, DSL, or bonded DIAL Internet Service Provider (ISP) sites (depending on service level score)	n/a[2]	n/a[3]
3. Mean time to respond (data centres and retailer sites)	15 minutes	$250	No	49
4. Rogers site network time to repair	6 hours	$50–$250 (depending on exceeded time)	Yes	n/a
5. Rogers DSL mean time to repair	4 hours	$1–$10 per incident (if exceeded by one to 6 minutes)	No	39
6. Data centre time to repair	4 hours	$1,000–$5,000 (depending on wait time)	No	2
7. Installs, moves, adds and changes credits	Installation must not be billed to Ontario Lottery and Gaming Corporation if Rogers fails to meet the agreed upon installation date			

1. In the last five years.
2. No instance of not meeting service level requirements in Rogers' Service Level report.
3. OLG incident-tracking tool identified over 70,000 incidents over the past five years.

service Category 2 (see **Figure 7**). However, according to OLG's incident-tracking tool, over 70,000 Category 2 incidents occurred in the past five years. Some incidents took more than a year to resolve.

Another example involves Canadian Bank Note, OLG's IT vendor for charitable gaming sites. OLG charges Canadian Bank Note penalty payments when service levels are not met for requirements such as service availability, speed to answer, first call resolution and time taken to restore service. We found 51 incidents in the past five years where service levels were not achieved for two service categories—28 for first call resolution and 23 for time taken to restore service—but no payments were charged or collected.

We noted that the reason OLG did not impose a penalty for these categories was because the penalty clause is not clearly defined in OLG's contract with Canadian Bank Note. The contract states that penalties can be imposed for critical incidents, but it lacks a clear-cut definition of "critical." As a consequence, OLG reviews only the number of incidents not resolved within the required time rather than reviewing the degree to which an incident is critical. This service-level agreement was signed in 2012 and has not been amended since to clarify the definition of "critical."

OLG Has Only One Internet Provider Serving Lottery Retailers with No Backup

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.

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.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) agrees with the recommendation and recognizes the importance of consistently enforcing the contractual obligations of its vendors. OLG is committed to establishing a robust process to identify and track underperformance, escalate its response to it, and apply appropriate penalties in accordance with vendor contracts.

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.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation will analyze the costs and benefits of acquiring a secondary lottery network provider and take action as appropriate.

4.1.5 OLG Extended or Renewed Strategic IT Contracts without Thoroughly Assessing Vendor Performance

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 such tools 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.

Figure 8 shows a summary of IT contracts OLG renewed with four vendors without doing performance assessments: Avatar Software Creations Inc., Omnigo Software, OR Computer Solutions and Plastic Mobile Inc.

Specifically, we found the following:

Avatar Software Creations Inc. (line of business: casinos)

OLG initially procured a software solution from Avatar for reporting on money laundering in August 2009. OLG renewed the service-level agreement with Avatar multiple times without reviewing its performance in meeting its service-level-agreement requirements.

In addition, OLG used single-source procurement, indicating in its business case that only this vendor was able to meet the regulatory and business requirements and provide ongoing software services and support. OLG told us it did not conduct research to support the single-sourcing, such as comparing what tools other Canadian lottery corporations procured for reporting on money laundering. We found that there are various IT software systems available from well-known technology companies like ORACLE and SAS that provide money-laundering-reporting capability.

Omnigo Software (line of business: casinos)

In 2008, OLG contracted with this vendor to provide facial recognition systems at all casinos. This contract was extended two subsequent times without assessing the vendor's performance against its service-level agreement. There have been about 1,500 incidents where facial detection issues occurred, yet OLG did not assess Omnigo's performance prior to the contract extensions.

OR Computer Solutions (line of business: lottery)

OLG extended the initial three-year agreement with OR Computer for another two years. However, OLG did not assess OR Computer's performance before extending the contract. OR Computer provides lottery terminal supplies—that is, papers, inks and parts for terminals, printers and scanners.

Figure 8: IT Contracts Renewed by Ontario Lottery and Gaming Corporation (OLG) without Vendor Performance Assessment

Prepared by the Office of the Auditor General of Ontario

Vendor	Service	Start Date	Original End Date	Extended End Date	Payment Start Date–Original End Date ($ million)	Payment Original End Date–Sep 5, 2019 ($ million)
Avatar Software	Software solutions for anti-money laundering reporting	Aug 18, 2009	Aug 17, 2012	Nov 30, 2020	0.1	1.4
Omnigo Software (iView Systems)	Manages self-excluded customers and security incidents for OLG gaming sites and resort casinos	Oct 13, 2008	Dec 31, 2013	Dec 11, 2020	2.7	4.1
OR Computer	Provides lottery terminal supplies	Jan 1, 2016	Dec 31, 2018	Dec 31, 2020	19.3	3.9
Plastic Mobile	Provides OLG lottery mobile application	Jan 1, 2014	Sep 14, 2016	Mar 31, 2021	2.5	7.8

Plastic Mobile Inc. (line of business: lottery)

OLG extended the agreement with Plastic Mobile three times since the original contract in January 2014. Plastic Mobile supports the web applications, platforms and databases that it developed for OLG. These critical services are not being monitored and evaluated by OLG to ensure that intended service delivery is provided successfully during the contract period.

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; and
- improve the existing procurement process by assessing whether a new tender for service is more appropriate than extending or renewing its contracts.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) agrees with this recommendation and will assess vendor performance prior to any contract renewal or extension. OLG is implementing thorough changes to its vendor management process, including establishing stronger performance management.

4.1.6 OLG Managers Not Clear on Responsibilities to Monitor IT Vendor Performance

OLG managers are responsible for monitoring that vendors adhere to performance requirements in their service-level agreements. One way they are to do this is to meet with vendors to review their performance at a specified frequency based on the vendor's classification (see **Figure 6**). We found that performance meetings were not taking place as required under contract. 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 addition, 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.

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; and
- develop guidance for OLG managers on what constitutes effective monitoring of vendor performance.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) agrees with the recommendation and understands the importance of ensuring its vendor management team fully understands roles and responsibilities in managing vendor partners. In addition, OLG is in the process of strengthening its tools and training for managers to effectively monitor vendor performance.

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

4.2.1 Need for Additional Penetration Testing to Reduce the Risk of Unauthorized Access to Personal Information

Organizations typically perform penetration testing on their IT systems to find security vulnerabilities. With respect to OLG, we found the following:

- Although OLG conducts regular vulnerability assessments, OLG has 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. According to industry best practices, such tests should be performed at least annually. In November 2018, the iGaming website was subject to a cyberattack causing PlayOLG.ca to be unavailable for approximately 16 hours. The attacker was never caught.
- OLG has also 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. In the past five years, there have been thousands of unsuccessful cyberattacks and attempts at OLG. Casino A was successfully attacked in November 2016.

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.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) recognizes the critical importance of safeguarding personal and confidential information and utilizes a comprehensive security framework that includes regular vulnerability assessments. OLG is committed to continual investment and will perform regular penetration testing of all critical IT systems.

4.2.2 Sensitive Personal Information Not Fully Safeguarded

OLG collects the personal information of customers for business purposes and regulatory compliance. This information can include a customer's name, birth date, race, address, gender, height, eye colour, hair colour, credit card information, banking information and personal identification numbers such as a driver's licence. The information is stored in OLG databases and is encrypted to prevent attackers from accessing it. However, OLG currently has seven employees who have 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.

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.

IT Division Does Not Keep Data Disposal Records as Required by Privacy Regulations

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.

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;
- review and where needed update its definition and classification of personal information annually; and
- ensure that data is disposed of according to the requirements of the *Freedom of Information and Protection of Privacy Act*.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) recognizes the critical importance of safeguarding personal and confidential information, and utilizes a comprehensive security framework that includes regular vulnerability assessments. OLG will review its definition and classification of personal information annually and update as required. OLG will also ensure that data is disposed of according to the requirements of the *Freedom of Information and Protection of Privacy Act*. OLG currently uses a number of controls that govern the collection and access of personal information, including encryption. OLG will review and restrict administrative access.

4.2.3 Casino Operators Not in Compliance with OLG Information Security Standards

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.

Major lessons learned from cyber incidents are also not shared across different casinos. Attempted data breaches at casinos and at OLG have remained steady in the past five years with an average of 300 cybersecurity attempts every year.

A data breach occurred in November 2016, when Casino A was hit with a cyberattack in 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:

- In May 2018, Casino B received a phishing email that became more targeted over three days as the unaware employees provided

information to the attacker. Accounts belonging to a total of six employees were compromised when user names and passwords were obtained by the hacker.

- In June 2019, Casino C received phishing emails. Ten employees from three affiliated casinos had their data compromised, which led to the attacker accessing confidential files in their email mailboxes.

These two incidents were similar to the Casino A incident, where employee awareness of these suspicious emails could have prevented the incident.

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; and
- ensure that all casinos deliver their established formal training programs for their staff to reduce the risk of successful cyberattacks.

RESPONSE FROM OLG

Consistent with its business practices and contractual obligations, the Ontario Lottery and Gaming Corporation (OLG) holds all its service providers accountable for fulfilling high standards of information security. OLG agrees with the recommendation and will ensure that all gaming sites comply with obligations for encryption of personal information as stipulated in casino operator contracts and deliver its established training programs to their staff to reduce the risk of cyberattacks.

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

We noted 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.

OLG uses a random-number-generator algorithm, which is a software formula that creates a sequence of numbers, to ensure that winning numbers are random and cannot be entered into the system fraudulently or predicted in advance. OLG contracts with an external vendor, Gaming Laboratories International, to assess the technical controls behind the system and evaluate the software formula to determine whether the system is able to generate random numbers suitable for its lottery products. We noted that the last technical assessment was performed in 2015.

An incident where lines of code were altered occurred across state lotteries in the United States. The former information security director of the Multi-State Lottery Association confessed in 2015 to inserting minimal lines of code to generate specific winning numbers on a specific day. While written in plain form with no attempt to hide its presence, the code did not change the size of the file and went undetected for over 10 years of reviews performed by the same external vendor as OLG uses, Gaming Laboratories International. A total of $24 million had been paid to illegitimate winners by the time the fraud was discovered.

To prevent such insider threats from affecting critical software, code reviews are accepted as a

form of best practice. Programmers who were not involved in the writing of the original code perform a review of the code to find any defects, such as malicious code or unintended functions.

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.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) agrees with the recommendation and will ensure the practice of source code review is included in its software development lifecycle process.

4.4 Comprehensive Disaster Recovery and Testing Strategy Needed

Organizations conduct disaster recovery exercises to determine whether they are able to restore IT operations in the event of a natural or man-made disaster such as power outages, cyberattacks and earthquakes. In a disaster recovery exercise, organizations test the availability of their IT operations by making them unavailable and moving the operations to an alternative site known as a backup facility. It is a best practice to conduct these exercises at least once a year for the entire IT network, which typically includes the collective technology infrastructure, including switches, routers, servers, IT systems and databases.

OLG has data centres in Toronto and Sault Ste. Marie where its data is stored from IT systems across all lines of its business. Disaster recovery strategies have been developed and tested for IT systems for each individual line of business. However, 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 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 (see **Figure 9** for OLG's targeted recovery times).

Classifications Determine whether IT System Tested for Disaster Recovery

OLG classifies its 186 systems according to how critical they are to its business operations (see **Figure 9**). 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

Figure 9: Disaster Recovery Classification for IT Systems and Test Frequency
Source of data: Ontario Lottery and Gaming Corporation

Classification	Test Frequency	Target Recovery Time	# of IT systems
Platinum	Annual	Less than 4 hours	34
Gold	Annual	4–24 hours	35
Silver	Annual	36 hours–7 days	42
Bronze	Not required	Best effort	9
Black/No profile	n/a	n/a	66
Total			**186**

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.

Based on our review of a number of systems, we noted some areas for improvement in OLG's disaster recovery planning and testing. For example:

- The central gaming management system (GMS) at OLG is classified as Platinum, meaning the GMS system should be recovered within four hours. We noted that the disaster recovery exercise for the GMS on March 6, 2019, was unsuccessful: the IT team was unable to recover the system within four hours. The system was not retested to verify successful recovery.
- Another significant IT system is the casino site GMS, which sends casino data to the central GMS at OLG. We found that the disaster recovery classifications were inconsistent across all casinos' site GMSs. For example, the system at Casino B is classified as Black, which means no targeted recovery time is in place, while Casino C is classified as Platinum, with a targeted recovery time in the event of an outage of less than four hours.
- We found that the Onyx IT system, which is used for call centre operations to respond to customers and retailers, is classified at the level where no review is performed, and therefore there is no disaster recovery process in place for it. We noted that the Onyx system's classification was last reviewed over 10 years ago. Industry best practice is for critical IT systems such as Onyx to be reviewed at least on an annual basis.

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;
- review its information systems classification on a periodic basis for consistency across OLG and casino IT systems; and
- retest the disaster recovery plan for its IT systems following each failed disaster recovery test.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) is committed to business continuity to ensure revenue streams and services to customers are protected. OLG is in the process of conducting a comprehensive third-party review of its key information technology systems and associated recovery plans to better address complex scenarios, including site-level disasters. OLG will review the recovery objectives of its information systems annually to ensure alignment with the needs of the business. We will ensure consistent classification is applied, documented and regularly reviewed across service providers.

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

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 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 account 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. For example:

- As a result of significant delays, one project had a $2-million cost overrun, making it 36% over its $5.6 million initial budget. The delays were mainly due to issues with the vendor's availability to participate in the system integration test. This resulted in additional costs for retaining OLG contractors and vendor consulting to support the integration.
- Another project associated with OLG's Internet gaming site, PlayOLG.ca, launched in January 2015, had a cost overrun of $3.6 million, making it 9% over its total budget. The project encountered higher-than-anticipated legal fees and other costs, including testing/validation costs as a result of business requirements not being clearly defined by OLG in its planning phase.

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.

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) recognizes the importance of robust project management to ensure that initiatives are completed on time and on budget. As a result of the audit, OLG has launched a new project control framework to strengthen oversight. OLG is also in the process of enhancing project management practices to improve project scheduling, budgeting and delivery. As well, OLG plans to upgrade the tools available to staff to better estimate and track project deliverables.

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

OLG has Casino Operating and Service Agreements (Agreements) with private-sector casino operators covering their administration and day-to-day operations of casino sites on OLG's behalf. In Ontario, 26 casinos in nine regions are operated by private-sector operators (see **Appendix 1**). Under the Agreements, OLG has the right to audit casinos to check if they are operating in compliance with contractual and regulatory requirements. The Agreements require casino operators to establish and monitor data regarding customers and gaming, IT security and cybersecurity of casino systems such as gaming management systems. Their operations are also subject to OLG's independent audits.

We found that OLG's Internal Risk and Audit Division has not performed the independent IT audits at all casinos as allowed under the Agreements. As shown in **Figure 10**, 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.

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.

Figure 10: Number of IT Audits Performed by Ontario Lottery and Gaming Corporation (OLG) Risk and Audit Division at Casinos

Source of data: Ontario Lottery and Gaming Corporation

Gaming Region	# of Casinos	# of IT Audits by OLG				
		2015	2016	2017	2018	2019
East	4	–	1	2	1	–
Southwest	6	–	–	1	2	–
North	3	1	–	–	1	–
Ottawa	1	–	–	–	–	1
Greater Toronto Area	3	–	–	1	–	3
West	4	1	–	–	–	–
Central	2	–	–	–	–	–
Niagara Falls	2	–	–	–	–	–
Windsor	1	–	–	–	–	–
Total	**26**	**2**	**1**	**4**	**4**	**4**

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

RESPONSE FROM OLG

The Ontario Lottery and Gaming Corporation (OLG) agrees with the recommendation and will review the current scope and frequency of audits to assess casino operators' performance of their IT responsibilities and implement adjustments to enhance its assurance coverage. OLG will formalize the process to review external audit reports and confirm corrective action has been taken.

Appendix 1: Casinos by Region and Casino Operator

Source of data: Ontario Lottery and Gaming Corporation

Gaming Region	Gaming Sites	Casino Operator	Privatization Dates
East	Shorelines Slots at Kawartha Downs	Great Canadian Gaming Corporation	Jan 11, 2016
	Shorelines Casino Thousand Islands		
	Shorelines Casino Belleville		
	Shorelines Casino Peterborough		
Southwest	Gateway Casinos Point Edward	Gateway Casinos and Entertainment Limited	May 9, 2017
	Gateway Casinos Dresden		
	Gateway Casinos Clinton		
	Gateway Casinos Woodstock		
	Gateway Casinos Hanover		
	Gateway Casinos London		
North	Gateway Casinos Sault Ste. Marie	Gateway Casinos and Entertainment Limited	May 30, 2017
	Gateway Casinos Thunder Bay		
	Gateway Casinos Sudbury		
Ottawa	Hard Rock Casino Ottawa	Hard Rock Ottawa Limited Partnership	Sep 12, 2017
Greater Toronto Area	Casino Woodbine	Ontario Gaming Greater Toronto Area Limited Partnership/Great Canadian Gaming Corporation	Jan 23, 2018
	Casino Ajax		
	Great Blue Heron Casino		
West	Elements Casino Grand River	Ontario Gaming West Greater Toronto Area Limited Partnership /Great Canadian Gaming Corporation	May 1, 2018
	Elements Casino Brantford		
	Elements Casino Flamboro		
	Elements Casino Mohawk		
Central	Casino Rama	Gateway Casinos and Entertainment Limited	Jul 18, 2018
	Gateway Casinos Innisfil		
Niagara Falls	Fallsview Casino Resort	Mohegan Gaming and Entertainment	Jun 11, 2019
	Casino Niagara		
Windsor	Caesars Windsor	Caesars Entertainment Windsor Limited	Current agreement expires on Jul 31, 2020

Appendix 2: Ontario Lottery and Gaming Corporation (OLG) IT Systems by Lines of Business

Source of data: Ontario Lottery and Gaming Corporation

Line of Business	Key IT Systems	Description
Casinos (Land-Based Gaming)	Bally Central Gaming Management System (GMS)	Bally Central Gaming Management System (GMS) is the key IT system being used at land-based gaming sites/casinos for accounting, financial management, reporting, and management of player data for land-based games. The main system is located at OLG, and land-based gaming sites have the Service Provider system. Developed by: External vendor (OLG Licensed Software) In use for: Three years (Central GMS). Implementation in progress (SP Site GMS) Last major upgrade: June 2018 Technology: Windows/MS SQL Server
	CasinoLink (legacy GMS)	CasinoLink is the legacy IT system being used at the land-based gaming sites/ casinos that is currently being retired. The system will be replaced with the above mentioned Bally GMS IT System by 2020. Developed by: External vendor (OLG Licensed Software) In use for: 10+ years Last major upgrade: August 2015 Technology: Windows / MS SQL Server
	iTrak iGWatch IP Facial Recognition System	iGWatch IP Facial Recognition System is used to identify voluntary self-excluders through surveillance cameras and matching with the facial recognition database as part of the Responsible Gambling program. Images of patrons that do not match the database are automatically deleted. Developed by: External vendor (OLG Licensed Software) In use for: Five+ years Last major upgrade: January 2019 Technology: Windows/MS SQL Server
	ContractHub (CLM, SRM)	ContractHub is used by the Land-Based Gaming team to track and manage the performance and obligations of service providers. It includes the following: • enhanced contract management • supplier relationship management • advanced workflows • supplier community access • financial transactions • encryption of sensitive data to meet OLG and government standards Contract Hub is also used by OLG Procurement for: • vendor good and service contract housing • auto-generated renewal and expiration notifications • encryption of sensitive data to meet OLG and government standards Developed by: External vendor (OLG Licensed Software) In use for: Five+ years Last major upgrade: November 2018 Technology: Apttus Salesforce

Line of Business	Key IT Systems	Description
Lottery	Online Lottery Gaming System (OLGS)	Manages all business logic and transaction integrity in selling tickets, picking winners and the payment of prizes. The system supports approximately 10,000 retailers across the province that record lottery-based customer transactions in the main gaming engines. Developed by: In-house In use for: Five+ years Last major upgrade: November 2018 Technology: Windows / MS SQL Server
	OLG Lottery Mobile App	The OLG Lottery Mobile App is used for ticket scanning, jackpot information, displaying winning numbers and coupons. Developed by: External vendor (OLG Licensed Software) In use for: Two+ years Last major upgrade: January 2019
iGaming (Internet Gaming)	PlayOLG.ca Gaming website	PlayOLG is the internet gaming platform provided by International Gaming Technology (IGT) as the third-party service provider. IGT manages front-line customer service, day-to-day hosting and the iGaming Solution software.
cGaming (Charitable Gaming)	Charitable gaming systems	IT systems for the charitable gaming centres are operated and managed by Canadian Bank Note as the third-party service provider.

Appendix 3: Audit Criteria

Prepared by the Office of the Auditor General of Ontario

1.	Governance and accountability structure is in place for IT functions and provide sufficient oversight over service providers key to IT operations.
2.	Effective oversight is in place to ensure that IT procurement process is managed in an efficient and cost-effective manner, in accordance with applicable legislation, regulations, directives and trade agreements.
3.	IT assets including technology equipment, software and hardware are effectively managed in an economical manner throughout the life cycle of the IT asset management process.
4.	Critical IT services are being delivered effectively and monitored to ensure intended outcomes are achieved in an economical manner.
5.	IT systems are in place to detect, prevent and mitigate anomalies and threats to Ontario Lottery and Gaming Corporation operations in a timely manner including the safeguarding of legislatively protected personal identifiable information.
6.	IT controls are in place to ensure fraudulent activities are being monitored and investigated. Accurate and timely data reporting is being performed in accordance with legislative and regulatory requirements.

Appendix 4: Actual IT Systems Outages and Impacts to Ontario Lottery and Gaming Corporation (OLG) Operations, January 2015–May 2019

Prepared by the Office of the Auditor General of Ontario

Line of Business	Vendor Name and IT System	# of Incidents	Resolution Time	Description	Risk	Impact
Casinos (Land-Based Gaming)	Avatar FINTRAC RTMS	680	Few hours to 23 days	Application unavailable to log in or save transactions. Error messages generated when users create a report for patron information.	Wrong patron information, incomplete reporting and anti-money laundering transactions not reported in a timely manner.	Inaccurate reporting, regulatory fines and system unavailability due to unresolved problems and incidents.
	Bally Gaming Management System (GMS)	3,000	Few hours to 600 days	Various issues with GMS and interfacing applications where the system does not sign up new patrons or search existing patrons on Casino Marketplace. Data from various casinos is not reconciled with the centralized data.	Application unavailability and inconsistent data reconciliation.	Negative customer experience and disruption to casino operations. Inconsistent data reconciliation for transactions and patron information resulting in inaccurate data reporting.
	IGT Casinolink and EZPay	3,000	Few hours to 95 days	Performance, capacity and availability controls are not adequately established and implemented. As a result, customers experience major delays in jackpot processing and ticket validation.	Inconsistent performance, capacity and availability with the system.	Negative customer experience and disruption to casino operations.
	NRT Cash Handling System for Automated Jackpot Dispensing Machines (AJM) and Customer Ticket Redemption (CTR)	2,900	Few hours to 7 days	AJM issues with processing jackpots. CTR bills jamming and cash dispense errors.	Inconsistent performance and availability with the system.	Negative customer experience and disruption to casino operations.
	Omnigo (iView) Facial Recognition System iTrak	1,500	Few hours to 200 days	Casinos not receiving facial recognition alerts.	Inability to prevent self-excluded patrons from entering casinos.	Litigation issues, revenue loss and public distrust.
Lottery	Plastic Mobile Lottery mobile application	290	Few hours to 34 days	Ticket checker failures.	Inability to check winning numbers.	Negative customer experience.