# Prize Payout Review Process Assessment

Audit Services

March 1, 2021

## Table of Contents

## Transmittal Letter

May 6, 2021

Martin Lampman
Director, Customer Support Operations
74 West Seymour
Kamloops, BC V2C 1E2

Dear Martin:

**Re: Prize Payout Review Process Assessment**

Attached is Audit Services' report on the Prize Payout Review Process Assessment. No exceptions were noted during our review.

We thank the management and staff of Player Services and Customer Support Centre for their cooperation and assistance during this engagement.

Sincerely,

s 22

Gurmit Aujla CPA, CA, CIA, CRISC, CRMA
Director, Internal Audit

cc: Peter ter Weeme, Chief Social Purpose Officer and VP Player Experience
Aidan Flynn, Manager, Player Services
Jennie Mundy, Manager, Customer Support Centre Accounts

## Introduction

In FY2020, Audit Services conducted a test of effectiveness on ILC Standards 12D – Retailer Fraud and 12I-Customer Complaints. The test included testing samples of prize claims to ensure the effectiveness of the prize payout control environment. Minor improvements were noted and discussed with management who requested we perform continuous reviews of prize claims to ensure the effectiveness of prize payout controls and processes. In December, BCLC Customer Support team began performing regular reviews of prize claims against Prize Payout Policy and Procedures. As a result, Audit Services agreed to assess the review process by Customer Support rather than performing continuous monitoring on prize claims.

## Statement of Objectives

The objective of this engagement was to provide reasonable assurance that the review process is adequate to ensure key controls in place are effective.

## Statement of Scope

The scope of this engagement included the assessment of the prize payout review process performed by Customer Support.

## Statement of Methodology

The following procedures were conducted:

- Inquiry and discussions with key personnel
- Review of procedures and practices
- Sample review of completed prize claim accuracy evaluations
- Identify and report opportunities for improvements

## Statement of Standards

We conducted our work in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform our work to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under review. This includes an assessment of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the objectives. We believe that our review provides a reasonable basis for our conclusions.

## Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes to key control areas during all engagements related to BCLC's core functions. Personnel changes can impact the control environment, effectiveness of key controls, and loss of risk and control knowledge. During this engagement, Audit Services confirmed that no role changes occurred that may impact the control processes under review.

## Conclusion

No exceptions were noted during our review.

## Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this engagement. Audit Services received full access to all resources and information required to complete this review.

# Cyber Security Incident Response Assessment

Audit Services

April 6, 2021

# Table of Contents

# Transmittal Letter

May 13, 2021

Mark Lane
Director, Cyber Security
74 West Seymour Street
Kamloops, BC V2C 1E2

Dear Mark:

**Re: Cyber Security Incident Response Assessment**

Attached is our report on the above review.

Audit Services assessed BCLC's Cyber Security Incident Response program against the Centre for Internet Security framework - Control 19[1]: Incident Response and Management with no exceptions noted. Opportunities to further improve the control environment have been discussed with management for further consideration.

In summary, our testing focused on the following aspects:

- Policies, procedures and standards,
- Business Continuity Planning and management oversight,
- Incidents reporting and follow up, and
- Training and communications.

We thank management and staff for their cooperation and assistance during this engagement.

Sincerely,

s 22

Gurmit Aujla CPA, CA, CIA, CRISC, CRMA
Director, Internal Audit

cc: Pat Davis, Chief Information Officer and VP, Business Technology
Marie-Noelle, Chief Compliance Officer and VP Legal, Compliance, Security

[1] Centre for Internet Security framework Control 19: https://www.cisecurity.org/controls/incident-response-and-management/

## Introduction

As BCLC continues its growth into digital gaming, it is critical to protect the organization's information and reputation by practicing an effective Cyber Security incident response program. This has become particularly relevant in the past year, because of the rise in cyber-attacks and the COVID-19 pandemic.

BCLC's Cyber Security department manages information security controls and performs incident response on behalf of the organization. This department established a program in 2019 to prevent, detect, respond to and recover from Cyber Security incidents. As included in our FY2021 audit plan, Audit Services performed a current state assessment of BCLC's Cyber Security Incident Program.

The goal of the Incident Response Program Assessment as defined by the Center for Internet Security[2] is to:

> *Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.*

## Statement of Objectives

The objective of this assessment was to review BCLC's Cyber Security incident response process and procedures against the Centre for Internet Security Controls framework – Control 19: Incident Response and Management.

## Statement of Scope

The scope of this engagement focused on BCLC's Cyber Security incident response program. The scope excluded privacy incident response and physical events within information security mandate, such as theft or loss of computers and mobile devices. Specifically, our testing included the following control areas (per the Centre for Internet Security Controls framework – Control 19: Incident Response and Management):

- 19.1 Document incident response procedures
- 19.2 Assign job titles and duties for incident response
- 19.3 Designate management personnel to support incident handling
- 19.4 Devise organization wide standards for reporting incidents
- 19.5 Maintain contact information for reporting security incidents
- 19.6 Publish information regarding reporting computer anomalies and incidents
- 19.7 Conduct periodic incident scenario sessions for personnel
- 19.8 Create incident scoring and prioritization schema

[2] The Center for Internet Security, Inc. (CIS) is a non-profit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber security; deliver world-class cyber security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.

## Statement of Methodology

Our methodology and approach included:

- Reviewing policy and process documentation.
- Conducting interviews with key personnel from Cyber Security team and Data Centre Operations.
- Identifying and reporting opportunities for enhancements.

## Statement of Standards

We conduct our engagements in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under review. An audit also includes assessments of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the audit objectives. We believe that our review provides a reasonable basis for our conclusions.

## Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes to key control areas during all engagements related to BCLC's core functions. Personnel changes can impact the control environment, effectiveness of key controls, and loss of risk and control knowledge. It was noted that there were no critical personnel changes in the Cyber Security team that administers this program.

## Conclusions

Based on our assessment against the Centre for Internet Security framework - Control 19: Incident Response and Management, we found that BCLC's Cyber Security Incident Response program aligned with this control framework and no exceptions were noted. Any considerations to further improve the control environment have been discussed with management.

Refer to Appendix 1 for details of our assessment.

## Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this review. Audit Services received full access to all resources and information required to complete this review.

# Appendix 1 – CIS Control Assessment

| Ref. | Control Areas | Assessment | Notes |
|---|---|---|---|
| 19.1 | **Document incident response procedures**<br>Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling / management. | 🟢 | BCLC Cyber Security team and s 15(1)(l) work together to perform incident response on a 24/7/365 basis.<br>s 15(1)(l)<br>of Work (SOW), BCLC Cyber Security incident response checklist and process flowcharts are the written documentation which define roles and responsibilities and procedures for incident handling. |
| 19.2 | **Assign Job titles and duties for incident response**<br>Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation throughout the incident through resolution. | 🟢 | BCLC Cyber Security team and s 15(1)(l) work together to perform incident response on a 24/7/365 basis. The specific roles and responsibilities are documented within the s 15(1)(l) SOW. On call staff from the two teams log incidents and track the handling process within s 15(1)(l). |
| 19.3 | **Designate management personnel to support incident handling**<br>Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles. | 🟢 | Director, Cyber Security oversees the Cyber incident responses with the Manager, Information Security being the backup. If both Director and Manager are away, the Chief Information Officer and Chief Compliance Officer are the executive level backups. |
| 19.4 | **Devise organization wide standards For reporting incidents**<br>Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. | 🟢 | According to BCLC's Appropriate Use Policy, "*all users must immediately report Information Security incidents*". BCLC users can report such incidents through s 15(1)(l), email, telephone or in person. s 15(1)(l) also reports anomalous events to the Cyber Security team and they follow the Service Level Agreements stated in the SOW. |
| 19.5 | **Maintain contact information for reporting security incidents**<br>Assemble and maintain information on third party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners. | 🟢 | Cyber Security team maintains a contact list for escalations and reporting security incidents. Specifically,<br>- For reporting a regular information security incident, the Cyber Security team works with s 15(1)(l), BT management and any involved parties.<br>- In case of a significant breach, BCLC Crisis Management Team, Executive, Board of Directors, and relevant business units are notified. If the external incident responses retainer needs to be engaged, Cyber Security and Legal Services will invoke the process.<br>- Occasionally, For information security incident with a privacy component, BCLC privacy team will be involved in the notification process. |
| 19.6 | **Publish Information Regarding Reporting Computer Anomalies and Incidents**<br>Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities. | 🟢 | Mandatory information security training is published and all BCLC employees are required to complete on an annual basis; follow-up for delinquent employees is completed by their managers. Employees can report cyber security incident through s 15(1)(l), email, telephone and in person. |
| 19.7 | **Conduct Periodic Incident Scenario Sessions for Personnel**<br>Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responder's technical capabilities using tools and data available to them. | 🟢 | Table top exercises are conducted at least annually. The last exercise was conducted in December 2020 with participants from Cyber Security, Data Centre Operations and other relevant Business Technology personnel. The exercise helped identify process gaps to further improve the Cyber Security Incident Response Program. |
| 19.8 | **Create Incident Scoring and Prioritization Schema**<br>Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures. | 🟢 | BCLC Cyber Security team and s 15(1)(l) established an incident scoring and prioritization schema, which uses scoring to define severity and escalation process. |

bclc

74 West Seymour Street
Kamloops, BC V2C 1E2

T 250 828 5500
F 250 828 5631

2940 Virtual Way
Vancouver, BC V5M 0A6

T 604 270 0649
www.bclc.com

April 30, 2021

Rod Toula
Interprovincial Lottery Corporation
40 Holly Street – 6th Floor
Toronto, ON M4S 3C3

Dear Mr. Toula:

Re: BCLC's Report on Compliance with ILC Control Standards

We have completed the audit of BCLC's compliance with the Interprovincial Lottery Corporation's ("ILC") Control Standards as required in the Regional Responsibilities (Section 1.2) of the ILC Policies and Procedures Manual.

Please find attached the completed Annual ILC Control Standards Audit report (referred to as Appendix 12 B).

The enclosed audit report is intended for the exclusive use of BCLC and ILC in assessing BCLC's compliance with the Control Standards as at March 31, 2021, and is not to be relied upon for any other purpose.

Yours truly

s 22

Gurmit Aujla, CPA, CA, CIA, CRISC, CRMA
Director, Audit Services

cc: Lynda Cavanaugh, Interim President and CEO, BCLC
Brad Desmarais, Chief Operating Officer, BCLC
Pat Davis, Chief Information Officer and VP, Business Technology, BCLC
Alan Kerr, Chief Financial Officer and VP, Corporate Services, BCLC

# Player Data Privacy Control Matrix & System Data Flow Review

Audit Services

## Table of Contents

## Transmittal Letter

June 30, 2021

Sarah Marshall
Data Governance Officer
2940 Virtual Way
Vancouver, BC V5M 0A6

Sydney Jones
Senior Manager, Privacy, FOI,
Information Governance
74 West Seymour Street
Kamloops, BC V2C 1E2

Kevin Sweeney
Director Enterprise Security and
Compliance
74 West Seymour Street
Kamloops, BC V2C 1E2

**Re: Player Data Privacy Control Matrix & System Data Flow Review**

Attached is Audit Services' report on the Player Data Privacy Control Matrix & System Data Flow review. This engagement commenced during the fourth quarter of FY2021 and is the first phase of a multi-phased Player Data Privacy audit approach.

This engagement served as a foundational piece to fully understand the control environment surrounding player information at BCLC. It should be noted activities performed by Audit Services' were intended to discover and document the current state of player data controls, including an enterprise-wide system data flow of personal player information. No testing or assurance work was performed in this phase, as this information will provide a framework to help determine areas for future assurance work. In this report, we have noted one moderate finding surrounding the lack of a formal data inventory or governance tool in regards to player data within BCLC systems. Opportunities to further strengthen key controls over BCLC's access, storage, and usage of player data were discussed with management. Audit Services plans to use the outcome of this engagement in future phases of our Player Data Privacy audit approach.

We would like to thank management and staff who assisted us during this review for their cooperation and support.

Sincerely,

s 22

Gurmit Aujla, CPA, CA, CIA, CRISC, CRMA
Director, Internal Audit

cc: Marie-Noëlle Savoie, Chief Compliance Officer and VP Legal, Compliance, Security
Peter ter Weeme, Chief Social Purpose Officer and VP, Player Experience

## Introduction

Following the completion of several Casino Service Provider Player Data Privacy reviews, Audit Services developed a comprehensive, multi-phased Player Data Privacy audit approach.

A large amount of player data is collected, used, and stored at BCLC during the normal course of business, and with this comes a significant inherent exposure to risk. The failure to properly protect player data could cause harm to BCLC's brand and reputation, unwanted exposure to our patrons, as well as subjection to financial penalties under applicable privacy laws and regulations (B.C. FIPPA and CASL [1]). As such, Audit Services needed to understand the control environment surrounding personal player information (PPI) contained within BCLC player data.

## Statement of Objectives

The objective of this engagement is to gain a broad understanding of BCLC's PPI landscape, specifically:

- *Collection:* what types of PPI are collected, and by who.
- *Usage:* how PPI is used within the organization.
- *Storage:* where and how PPI is stored.
- *Sharing:* what disclosure, transmission, or transfer of PPI is occurring.
- *Security:* BCLC's privacy processes and controls related to the protection of PPI.

## Statement of Scope

The scope of this engagement assessed structured PPI within identified BCLC internal systems, applications, and the enterprise data warehouse. These included:

- Casino Systems s 15(1)(l)
- eGaming Systems s 15(1)(l)
- s 15(1)(l)
- s 15(1)(l) (components for both Encore, PlayNow);
- s 15(1)(l)
- s 15(1)(l) and
- Casino Reporting System s 15(1)(l)

The scope did not include unstructured PPI within BCLC's enterprise content management structure of business applications, as well as PPI at Casino Service Providers and third party vendors.

[1] FIPPA refers to BC's *Freedom of Information and Protection of Privacy Act* while CASL is *Canada's Anti-Spam Legislation*

## Statement of Methodology

This engagement was based on the premise that management is responsible for identifying its business risks and managing them by designing and maintaining a system of internal controls that mitigates these risks. The role of the auditor is to assess these management controls and determine whether they are adequate and effective.

Our methodology and approach included:

- Interviews, inquiries, and observations with key BCLC personnel;
- Review of privacy procedures and practices at BCLC;
- Identification of potential areas of concern or weakness;
- Preparing a flowchart demonstrating the process flows, mapping player data attributes, pinpointing key controls, and highlighting the risks;
- Validating the results with key stakeholders; and
- Providing recommendations to address and mitigate risks.

## Statement of Audit Standards

We conducted our engagement in accordance with professional standards issued by the Institute of Internal Auditors. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws, rules and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

## Conclusion

Audit Services gathered information and prepared a process flow map of PPI within BCLC's internal systems, applications, and the EDW. This included flowcharting how the systems integrate with each other, as well as the points where PPI enters the organization. Audit Services interviewed system owners, obtaining resource documents to understand the attributes of the PPI captured by the various systems, applications, and the EDW. In addition, we outlined where PPI is retained within the organization, and the number of employees with access to the data. This deliverable has proven to be a valuable input for the organization, and a good resource for information on the relationship between BCLC's internal systems and their respective player data attributes. BCLC's Cyber Security team has agreed to host the final flowchart deliverable, allowing others in the organization to leverage this useful information and to facilitate updates to keep it current as required. Audit Services has presented our findings to management and are defining the next phase of our Player Data Privacy review.

## Acknowledgements

We wish to thank management and staff for their participation, assistance and cooperation during this review. Audit Services received full access to all resources and information required to complete this engagement.

# Findings

The following is the finding that we identified during our fieldwork, along with associated recommendations to address the issue. To assist management in prioritizing action plans in response to our recommendations, we have categorized the issue by level of risk, using the following scale:

- High – Issue should be addressed and resolved immediately;
- Moderate – Issue requires management attention and should be addressed and resolved within a reasonable time period; or
- Low – Issue is of lesser significance that is administrative in nature.

## Finding (Moderate)

Audit Services noted that an inventory of PPI has not previously been consolidated, and there is no established process or tool to capture and maintain this information and keep it current.

## Recommendation

Audit Services recommends maintaining a complete and current inventory of PPI at BCLC, noting where it is collected, secured, accessed, and how it is used, in order to maintain protection of this information and support the ongoing development of a player data strategy.

## Management Response

Management agrees and supports Audit Services' finding and recommendation. As a near-term solution, management will consider various processes and control mechanisms to support the maintenance of a complete and current inventory of PPI at BCLC. We look forward to working closely with Audit Services on developing these in Phase Two and exploring solutions to develop a multi-phased approach long term.