Cloud Security Assurance

Audit Services

August 5, 2021

Table of Contents

Transmittal Letter

September 29, 2021

Ash Kosmadia
Director Technology Platform Enablement
74 West Seymour Street
Kamloops, BC V2C 1E2

Dear Mr. Kosmadia:

Re: Cloud Security Controls Assessment – Amazon Web Services

Attached is our report on the above review.

Audit Services assessed BCLC's Amazon Web Services (AWS) cloud platform against ISACA[1]'s 2019 Amazon Web Services Audit Program. Opportunities to further improve the control environment have been discussed with management for further consideration.

In summary, our testing focused on the following aspects:

- Logical access controls
- Data encryption controls

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
Don Lacey, Director Technology Platform Enablement (Retiring)
Craig Ozubko, Product Owner Platform Enablement

[1] ISACA is an internationally recognized professional association focused on IT governance. It provides a centralized source of information and guidance on assurances, governance, risk, security and emerging technology audits

Introduction

The utilization of cloud computing services such as Amazon Web Services (AWS) is growing rapidly and playing a strategic role in provisioning technology solutions for BCLC. It significantly reduces the total cost of technology ownership and provides efficiencies on the agile delivery of technological products.

Given that the cloud computing platform can host sensitive information, proprietary data and gaming information, it is crucial to assure a robust internal control structure for this platform. ISACA[1] (Information Systems Audit and Control Association) published an audit program for auditing an AWS cloud platform. Audit Services performed a current state assessment of BCLC's control environment using this ISACA AWS audit program.

Statement of Objectives

The objective of this assessment was to review the control environment of BCLC's AWS cloud computing service against the control requirements published by ISACA[1] on this specific area.

Statement of Scope

Our scope covers the logical access controls and data encryption controls. Specifically, we assessed the following control areas, as per ISACA's AWS Audit Program:

For logical access controls:

- Securing root access
- Establishing role-based access
- Segregating duties
- Restricting Administrative Toolsets
- Removing access
- Assessing access roles and permissions
- Delegating access to external AWS accounts
- Controlling Access to cryptographic keys
- Enforcing Session timeouts
- System use notifications

For Data encryption controls:

- Defining encryption requirements
- Encrypting Data by Classification
- Securing remote connectivity
- Detecting misconfigured encryption

[1] ISACA is an internationally recognized professional association focused on IT governance. It provides a centralized source of information and guidance on assurances, governance, risk, security and emerging technology audits.

Statement of Methodology

Our methodology and approach included:

- Reviewing policy and process documentation;
- Conducting interviews with key personnel from Business Technology teams;
- Performing walk-through of process and control activities related to AWS;
- 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 Business Technology team that administers this program.

Conclusions

Based on our assessment, we found that the logical access controls and data encryption controls for BCLC's AWS cloud platform compliant with the control requirements recommendation by ISACA.

s 15(1)

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 – AWS Audit Program by ISACA

Amazon Web Services® (AWS®) Audit Program
Logical Access Controls
ISACA 2019

Process Sub-area	***Control Objectives***	***Controls***	***Assessment Result***
Securing Root Account Access	Accountability and security of AWS-based business functions are achieved through restricted access to AWS root accounts.	The enterprise disables AWS root account access and utilizes a secured password vault to control use of account credentials.	Pass
	The enterprise maintains integrity of AWS root accounts by implementing multifactor authentication.	AWS root accounts are configured to require multifactor authentication before they may be used.	Pass
Establishing Role-based Access	Data confidentiality is ensured by managing access based on the level of access needed for users or network functions to perform their intended roles.	The enterprise has developed and configured access roles to provision users or network services according to the principle of least privilege.	Pass
Segregating Duties	The enterprise maintains the integrity and confidentiality of AWS applications through identification and reduction of conflicting access.	The enterprise has developed network-access baselines based on position responsibilities and generates alerts when modifications occur.	Pass
Restricting Administrative Toolsets	The enterprise maintains confidentiality and integrity of the environment by limiting administrative tools available to personnel.	The ability to administer AWS applications is limited to authorized tools and users.	Pass
Removing Access	Once identified, inappropriate access (e.g., access that no longer serves a business need) is completely removed in a timely manner.	AWS accounts are disabled after an enterprise-defined period of inactivity, then are removed, if necessary.	Pass
Segregating Duties	The enterprise ensures data confidentiality and security through password protection of user accounts accessing AWS applications.	The system enforces password policies which • Require minimum password length • Constrain use of historical passwords • Require predefined password complexity	Pass
Assessing Access Roles & Permissions	The enterprise maintains appropriateness of access roles and related permissions policies through ongoing reviews and real-time monitoring.	s 15(1) alarms are configured to alert the appropriate enterprise-defined department or individuals when AWS access roles or permissions are created or modified. Management reviews appropriateness of access provided to AWS access roles and associated permissions on a regular basis, as defined by the enterprise.	Pass
Delegating Access to External AWS Accounts	The enterprise enforces AWS application confidentiality and integrity by requiring multifactor authentication.	Privileged users and application programming interfaces (API) are required to authenticate to the network using multifactor authentication (MFA).	Pass
	Management of external access to AWS applications through authorization ensures that actions taken are restricted to actions that have been approved for that particular role.	The enterprise creates and manages identity and access management (IAM) roles that external enterprises use to access AWS applications and related resources. Access is terminated in a timely manner when there is no longer a business need for the access.	Pass
Controlling Access to Cryptographic Keys	The enterprise maintains confidentiality and integrity of cryptographic information by restricting access to appropriate individuals.	The enterprise grants s 15(1) access to personnel (based on job responsibilities) and implements access based on the principle of least-privileged. The enterprise utilizes s 15(1) to monitor s 15(1) calls for appropriateness.	Pass
Enforcing Session Timeouts	The enterprise ensures integrity of AWS application sessions by enforcing session timeouts.	AWS user sessions time out after an interval defined by the enterprise.	Pass
System Use Notifications	The enterprise ensures security and appropriate use of its network by defining and communicating expected behavior to users prior to granting user access.	A system-use notification, outlining acceptable use, is presented to users and requires their acknowledgement before they are granted AWS application access.	N/A for BCLC

Appendix 1 – AWS Audit Program by ISACA (Continued)

Amazon Web Services® (AWS®) Audit Program
Data Encryption Controls
2019 ISACA

Process Sub-area	***Control Objectives***	***Controls***	***Assessment Result***
Defining Encryption Requirements	The enterprise applies appropriate encryption to individual data stores that is commensurate with business requirements	The enterprise requires a minimum of s 15(1) encryption for data at rest and in transit.	Pass
Encrypting Data by Classification	The enterprise maintains data confidentiality through the application of encryption, as defined by data classification requirements.	The enterprise secures AWS data containers (S3 buckets, RedShift clusters, etc.), using client-side and server-side encryption.	Pass
Securing Remote Connectivity	The enterprise maintains data confidentiality and integrity for external network sources and destinations.	The enterprise requires encrypted connections for communications with external destinations.	Pass
Detecting Misconfigured Encryption	The enterprise maintains integrity of encryption status through use of monitoring.	The enterprise has developed capabilities to identify and respond to encryption failures or misconfigurations in a timely manner.	Pass

GameSense Performance Assessment Report

September 21, 2021

Jamie Wiebe
Director, Player Health
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Ms. Wiebe:

Re: GameSense Performance Assessment – Casino Reopening

BACKGROUND

Attached is Audit Services' consolidated GameSense Performance Assessment, performed at 30 sites surrounding the date casinos reopened on July 1, 2021.

The scope of our assessment focused on the following questions:

Locational GameSense Information Centre (GSIC) elements:

- Does the GameSense location have the required furnishings?
- Is the GameSense location stocked with appropriate materials?
- Is the GameSense location easy to locate within Casino property?
- Were all available QR codes functioning?

GameSense Advisor (GSA) elements:

- Was the GSA availability schedule easy to locate?
- If the GSA was on shift:
  - Was the GSA easy to find if not in the GameSense Information Center?
  - Was the GSA easy to identify and outfitted differently than the other gaming venue staff?
  - Did the GSA look available and approachable?

FINDINGS

Audit Services determined that many of the issues noted below were due to the timing of testing; some GSIC, as well as casinos in general, were going through rapid renovation just prior to reopening their doors to the public. This meant many GSIC were not fully setup prior to opening. We expect to re-test these sites later in FY2022.

Additionally, we coordinated with GPEB, who conducted testing on behalf of Audit Services at some of the northern gaming sites. This reduced travel and associated carbon footprint for testing destinations that require several days of travel.

This consolidated report card below summarizes the work completed. We have communicated detailed reporting to management throughout the reopening process. Audit Services will conduct additional GameSense Performance Assessments throughout FY2022, continuing to use this streamlined reporting system to ensure the Director of Player Health is immediately aware of any major/serious issues.

We thank the management and staff of Player Health 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

CONSOLIDATED REPORT CARD SUMMARY

Site	Date Tested	Status
Billy Barker[1]	2021-Jul-20	✓
Cascades Kamloops	2021-Jun-21	✓
Cascades Langley	2021-Jun-30	✓
Cascades Penticton	2021-Jun-21	↻
Casino Nanaimo	2021-Jun-30	✓
Chances Abbotsford	2021-Jul-14	✓
Chances Campbell River	2021-Jul-13	✓
Chances Courtenay	2021-Jul-13	✓
Chances Cowichan	2021-Jul-14	✓
Chances Kamloops	2021-Jun-21	✓
Chances Kelowna	2021-Jun-22	↻
Chances Maple Ridge	2021-Jun-30	✓
Chances Mission	2021-Jun-30	↻
Chances Prince Rupert [1]	2021-Jul-15	✓
Chances RimRock	2021-Jul-14	✓
Chances Salmon Arm	2021-Jun-21	✓
Chances Signal Point [1]	2021-Jul-21	✓
Chances Squamish	2021-Jun-23	✓
Chances Terrace [1]	2021-Jul-14	✓
Elements Chilliwack	2021-Jun-30	✓
Elements Surrey	2021-Jun-30	✓
Elements Victoria	2021-Jul-14	✓

[1] For four sites, Billy Barker, Prince Rupert, Signal Point and Terrace, Audit Services leveraged GPEB's audit presence at these northern sites with GPEB performing the audit procedures.

Note: GPEB does not express an assurance conclusion on the tests performed. Audit Services reviewed GPEB's work based on the procedures performed, validated findings (if any) and drew our own conclusions.

Site	Date Tested	Status
Grand Villa Casino	2021-Jun-28	↻
Hard Rock Casino	2021-Jun-29	↻
Hastings Racecourse	2021-Jun-29	↻
Lake City Vernon	2021-Jun-21	✓
Parq Casino	2021-Jun-28	✓
Playtime Kelowna	2021-Jun-22	↻
River Rock Casino	2021-Jun-28	↻
Starlight Casino	2021-Jun-29	↻

LEGEND

Follow-Up Not Required	Follow-Up Required
✓	↻

Testing Notes:

Cascades Penticton – updated GSIC not been set up due to reopening renovations

Chances Kelowna – updated GSIC not been set up due to reopening renovations

Chances Mission – GSIC has received no updates (i.e. branding, furnishings, etc.)

Grand Villa – GSIC has received no updates (i.e. branding, furnishings, etc.), did not have appropriate materials stocked on date of visit (shelf was empty)

Hard Rock Casino – GSIC has received no updates (i.e. branding, furnishings, etc.), did not have appropriate materials stocked on date of visit (shelf was empty), and is hard to locate

Hastings Racecourse – GSIC has received no updates (i.e. branding, furnishings, etc.) and did not have appropriate materials stocked on date of visit (shelf was empty); staff note they plan on relocating after reopening

Playtime Kelowna – updated GSIC not been set up due to reopening renovations

River Rock Casino – GSIC has received no updates (i.e. branding, furnishings, etc.), did not have appropriate materials stocked on date of visit (shelf was empty), and is very hard to locate

Starlight Casino – GSIC did not have appropriate materials stocked on date of visit (shelf was empty)

**Audit Services noted an issue with the QR code for the main GameSense brochures during the pre-opening testing of all sites; the QR code for the corresponding website had expired, and we received a message saying that the campaign had been disabled. This was raised to the Director of Player Health pre-opening, and Audit Services noted the code was reactivated and remedied as of July 13, 2021 on sites tested subsequent to this date.*

Consolidated RTP Audit Report Card

September 27, 2021

Garth Pieper
Director, Casino Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Pieper:

Re: Return to Player Settings Audit – Casino Reopening

BACKGROUND

Attached is Audit Services' consolidated report for the Return to Player (RTP) Settings Audit, which was performed at 35 sites surrounding the date casinos reopened on July 1, 2021.

This audit is part of Casino Back to Business Assurance engagement on the Annual Audit Plan, approved by the Audit Committee for Fiscal Year 2022.

SCOPE AND OBJECTIVE

The scope includes all enabled machine (some machines were disabled to meet social distance requirements) at Casinos and Community Gaming Centers in BC.

The objective of this engagement is to examine the RTP settings for a sample of slot machines at the gaming facilities and verify that they were configured consistently with management's expectation.

FINDINGS

In conclusion, we identified seven error out of the 4,682 machines (53% of the total enabled machines) tested in 35[1] sites. The technicians on site corrected the settings errors immediately and we validated the change to ensure the correct rate was entered; this is the standard practice with RTP auditing.

This consolidated report card is intended to be a summary of the work completed; detailed reporting has been communicated to management throughout the reopening process.

We thank the management and staff of Casino Operations for their cooperation and assistance during this audit.

Sincerely,

s 22

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

cc: Brad Desmarais, Chief Operating Officer

[1] Audit Services coordinated with GPEB auditors, who performed RTP testing at nine remote sites during their planned audits; testing samples selected by Audit Services. GPEB does not provide an assurance opinion on work performed.

CONSOLIDATED REPORT CARD SUMMARY

Site	Date Tested	Status	# of Errors
Billy Barker *(tested by GPEB)*	July 20, 2021	✓	
Cascades Kamloops	June 21, 2021	✓	
Cascades Langley	June 30, 2021	✗	2
Cascades Penticton	July 21, 2021	✓	
Casino Nanaimo	June 30, 2021	✓	
Chances Abbotsford	July 14, 2021	✗	1
Chances Campbell River	July 13, 2021	✓	
Chances Courtenay	July 13, 2021	✓	
Chances Cowichan	July 14, 2021	✓	
Chances Kamloops	June 21, 2021	✓	
Chances Kelowna	June 22, 2021	✓	
Chances Maple Ridge	June 30, 2021	✗	2
Chances Mission	June 30, 2021	✓	
Chances Prince Rupert *(tested by GPEB)*	July 15, 2021	✓	
Chances RimRock	July 14, 2021	✓	
Chances Salmon Arm	June 21, 2021	✓	
Chances Signal Point *(tested by GPEB)*	July 21, 2021	✓	
Chances Squamish	June 23, 2021	✓	
Chances Terrace *(tested by GPEB)*	July 14, 2021	✓	
Elements Chilliwack	June 30, 2021	✓	
Elements Surrey	June 30, 2021	✓	
Elements Victoria	July 14, 2021	✓	
Grand Villa Casino	June 28, 2021	✓	
Hard Rock Casino	June 29, 2021	✓	
Hastings Racecourse	June 29, 2021	✗	1
Lake City Vernon	June 21, 2021	✓	
Parq Casino	June 28, 2021	✓	

Site	Date Tested	Status	# of Errors
Playtime Kelowna	June 22, 2021	✓	
River Rock Casino	June 28, 2021	✓	
Starlight Casino	June 29, 2021	✓	
Chances Dawson Creek *(tested by GPEB)*	August 11, 2021	✓	
Chances Fort St. John *(tested by GPEB)*	August 12, 2021	✓	
Casino of the Rockies *(tested by GPEB)*	August 25, 2021	✗	1
Chances Castlegar *(tested by GPEB)*	August 26, 2021	✓	
Treasure Cove *(tested by GPEB)*	September 3, 2021	✓	

LEGEND

Follow-Up Not Required	Follow-Up Required	Error(s) Noted
✓	↻	✗

Testing Notes:

The seven errors noted above were immediately fixed by on site technicians. Audit Services validated the corrections to ensure that the RTP were set accurately.

Casino Reopening Cyber Security Assessment Report

September 29, 2021

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

Dear Mr. Lane:

Re: Cyber Security Site Testing – Casino Reopening

Attached is Audit Services' consolidated Cyber Security Performance Assessment, performed at 26 sites surrounding the date casinos reopened on July 1, 2021. With the casinos and Community Gaming Centers (CGC) closed, this provided an opportunity to create an audit program (supported by Cyber Security, PCI Compliance and Casino Operations) which could test, and ultimately enhance, the control environment moving forward. Audit Services also utilized Public Health Office (PHO) directives to frame the final testing attributes.

BACKGROUND

In preparation for the July 1, 2021 reopening, Audit Services collaborated with the Cyber Security team with the goal of creating a series of onsite, repeatable tests which would test the current control environment. We designed the following areas of testing with this goal:

- Inspect all workstations and related peripheral devices for security and access controls
- Inspect slot machine and related network cabling
- Inspect table games GMS devices and related secure cabling
- Capture and review all Wi-Fi access points
- Server room controls testing with included:
  - server cabling
  - security and cleanliness
  - physical door controls
- Inspect Lottery sales location controls (access, network cabling) at sites where available

OBSERVATIONS

We communicated all data gathered immediately to BCLC's Cyber Security division. This allowed Casino Operations to conduct any additional investigation and remediation. Audit Services determined that observations were due to a few common issues:

- Prior to July 1, 2021, sites were not open to the public and some BCLC Slot Technician room doors remained unlocked/pinned open. Best practice is to keep the Technician door locked at all times. Testing which occurred after July 1, 2021 (public permitted in casinos) did not have this observation;

- Slot floors have been re-arranged to create more distance between each machine (in line with PHO directive), and in some locations this resulted in network cables/devices becoming visible and could be accessed by the public. Remediation through either re-cabling and/or physical barriers were implemented at all sites as soon as the finding was communicated to Casino Operations; and

- Sites had many PHO projects running concurrently, and with limited space inside tech rooms, items were stored within the server rooms. Best practice is to keep server rooms clear of all materials for optimal cooling/fire suppression.

REMEDIATION AND REPORTING

Audit Services coordinated the onsite testing with Cyber Security in-person at River Rock and Parq Casino to ensure testing, reporting and communication strategies were in place and consistent. Casino Operations, including onsite techs and Managers of Business Operation, worked to ensure all findings were remediated as soon as possible.

We provided this consolidated report card summarizing the work completed; detailed reporting has been communicated to Cyber Security and Casino Operations. Audit Services will conduct additional Cyber Security Site Performance Assessments throughout FY2022, continuing to use this streamlined reporting system to ensure the Cyber Security division is immediately advised of all major/serious issues.

A sincere thank you to Cyber Security and Casino Operations divisions and staff for the execution of this engagement with such a rapidly changing control environment and aggressive timeline.

Sincerely,

s 22

[redacted] SC, CRMA
Director, Internal Audit

cc: Garth Pieper, Director Casino Operations
Eric Tong, Senior Specialist Privacy and Security

CONSOLIDATED REPORT CARD SUMMARY

Site	Date Tested	Status
Cascades Kamloops	2021-June-21	✓
Cascades Langley	2021-June-30	✓
Cascades Penticton	2021-June-21	✓
Casino Nanaimo	2021-June-30	✓
Chances Abbotsford	2021-July-14	✓
Chances Courtenay	2021-July-13	↻
Chances Cowichan	2021-July-14	✓
Chances Kamloops	2021-June-21	✓
Chances Kelowna	2021-June-22	✓
Chances Maple Ridge	2021-June-30	↻
Chances Mission	2021-June-30	↻
Chances RimRock	2021-July-14	✓
Chances Salmon Arm	2021-June-21	↻
Chances Squamish	2021-June-23	✓
Elements Chilliwack	2021-June-30	✓
Elements Surrey	2021-June-30	↻
Elements Victoria	2021-July-14	✓
Grand Villa Casino	2021-June-28	↻
Hard Rock Casino	2021-June-29	↻
Hastings Racecourse	2021-June-29	↻
Lake City Vernon	2021-June-21	✓
Parq Casino	2021-June-28	↻
Playtime Kelowna	2021-June-22	✓
River Rock Casino	2021-June-28	✓
Starlight Casino	2021-June-29	✓

LEGEND

Follow-Up Not Required	Follow-Up Required
✓	↻