Return to Player Settings Audit – Q4 Starlight Casino

Audit Services

February 4, 2020

Table of Contents

Transmittal Letter 1

Introduction 2

Statement of Objectives 2

Statement of Scope 2

Statement of Methodology 2

Statement of Audit Standards 2

Personnel Changes in Key Control Areas 3

Conclusion 3

Acknowledgements 3

Transmittal Letter

March 23, 2020

Tom Maryschak
Senior Manager Casino Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Maryschak:

Re: Return to Player (RTP) Audit – Starlight Casino

Attached is the Audit Services' report on the RTP testing which occurred at Starlight Casino on February 4, 2020. The scope of our audit focused specifically on the RTP settings at Starlight Casino for a selected sample of slot machines.

During the course of our work conducted at Starlight Casino, we noted that all 235 machines tested had their RTP settings set correctly. In total, Starlight Casino has 959 slot machines.

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

Sincerely,
s 22

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

cc: Kevin Sweeney, Director Security, Privacy and Compliance
Brett Lawrence, Regional Manager, Operations
Brian Pay, Manager, Business Operations

Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings at Starlight Casino on randomly selected slot machines. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020.

Statement of Methodology

Our methodology and approach included:

- Testing RTPs of randomly selected slot machines
- Confirming the RTP from slot machines to Master Data: rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)
- Interviews & inquiries
- Identifying process weaknesses, risks and controls

Statement of Audit Standards

We conducted our audit 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.

Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Starlight Casino, BCLC staffing component consists of a Manager Business Operations, one Senior Technician and seven Technicians.

We noted during this audit that three new employees joined the Starlight's BCLC team during fiscal 2019-2020. Two individuals are existing BCLC employees who transferred from different sites, and the other individual was hired externally but with similar gaming experience. As a result, these personnel changes do not impact the control environment or control effectiveness.

Conclusion

Audit Services found no RTP exceptions in the 235 machines tested on February 4, 2020.

Acknowledgements

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

Return to Player Settings Audit – Q4 Chances Squamish

Audit Services

February 13, 2020

Table of Contents

Transmittal Letter 1

Introduction 2

Statement of Objectives 2

Statement of Scope 2

Statement of Methodology 2

Statement of Audit Standards 2

Personnel Changes in Key Control Areas 3

Conclusion 3

Acknowledgements 3

Transmittal Letter

March 23, 2020

Tom Maryschak
Senior Manager Casino Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Maryschak:

Re: Return to Player (RTP) Audit – Chances Squamish

Attached is the Audit Services' report on the RTP testing which occurred at Chances Squamish on February 13, 2020. The scope of our audit focused specifically on the RTP settings at Chances Squamish for all slot machines.

During the course of our work conducted at Chances Squamish, we noted that all 97 machines tested had their RTP settings set correctly. In total, Chances Squamish has 97 slot machines.

We thank the management and staff of the Chances Squamish for their cooperation and assistance during this audit.

Sincerely,
s 22

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

cc: Kevin Sweeney, Director Security, Privacy and Compliance
Ken Bach, Regional Manager, Operations
Ray Palumbo, Manager, Business Operations

Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings on all slot machines at the Chances Squamish location. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020. This engagement occurs annually.

Statement of Methodology

Our methodology and approach included:

- Testing RTPs of slot machines
- Confirming the RTP from slot machines to Master Data: SharePoint/rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)
- Interviews & inquiries
- Identifying process weaknesses, risks and controls

Statement of Audit Standards

We conducted our audit 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.

Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Chances Squamish, BCLC staffing component consists of a Manager Business Operations and one Senior Technician. We noted during this audit that the BCLC staff at Chances Squamish had a minimal staff turnover rate.

Conclusion

Audit Services found no RTP exceptions in the 97 machines tested on February 13, 2020.

Acknowledgements

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

Return to Player Settings Audit – Q4 Hard Rock Casino

Audit Services

February 20, 2020

Table of Contents

Transmittal Letter 1

Introduction 2

Statement of Objectives 2

Statement of Scope 2

Statement of Methodology 2

Statement of Audit Standards 2

Personnel Changes in Key Control Areas 3

Conclusion 3

Acknowledgements 3

Transmittal Letter

March 23, 2020

Tom Maryschak
Senior Manager Casino Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Maryschak:

Re: Return to Player (RTP) Audit – Hard Rock Casino

Attached is the Audit Services' report on the RTP testing which occurred at Hard Rock Casino on February 20, 2020. The scope of our audit focused specifically on the RTP settings at Hard Rock Casino for a selected sample of slot machines.

During the course of our work conducted at Hard Rock Casino, we noted that all 200 machines tested had their RTP settings set correctly. In total, Hard Rock Casino has 997 slot machines.

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

Sincerely,
s 22

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

cc: Kevin Sweeney, Director Security, Privacy and Compliance
Bal Bains, Regional Manager, Operations
Paul Bystrowski, Manager, Business Operations

Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings on all slot machines at the Hard Rock Casino location. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020. This engagement occurs annually.

Statement of Methodology

Our methodology and approach included:

- Testing RTPs of slot machines
- Confirming the RTP from slot machines to Master Data: SharePoint/rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)
- Interviews & inquiries
- Identifying process weaknesses, risks and controls

Statement of Audit Standards

We conducted our audit 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.

Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Hard Rock Casino, BCLC staffing component consists of a Manager Business Operations, one Senior Technician, and multiple full-time technicians. We noted during this audit that the BCLC staff at Hard Rock Casino had a minimal staff turnover rate.

Conclusion

Audit Services found no RTP exceptions in the 200 machines tested on February 20, 2020.

Acknowledgements

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

Return to Player Settings Audit – Q4 Chances Kamloops

Audit Services

February 21, 2020

Table of Contents

Transmittal Letter 1

Introduction 2

Statement of Objectives 2

Statement of Scope 2

Statement of Methodology 2

Statement of Audit Standards 2

Personnel Changes in Key Control Areas 3

Conclusion 3

Acknowledgements 3

Transmittal Letter

March 23, 2020

Tom Maryschak
Senior Manager Casino Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Maryschak:

Re: Return to Player (RTP) Audit – Chances Kamloops

Attached is the Audit Services' report on the RTP testing which occurred at Chances Kamloops on February 21, 2020. The scope of our audit focused specifically on the RTP settings at Chances Kamloops for a selected sample of slot machines.

During the course of our work conducted at Chances Kamloops, we noted that all 99 machines tested had their RTP settings set correctly. In total, Chances Kamloops has 200 slot machines.

We thank the management and staff of Kamloops Chances for their cooperation and assistance during this audit.

Sincerely,

s 22

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

cc: Kevin Sweeney, Director Security, Privacy and Compliance
Brett Lawrence, Regional Manager, Operations
Richard Frater, Manager, Business Operations

Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings at Chances Kamloops on randomly selected slot machines. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020.

Statement of Methodology

Our methodology and approach included:

- Testing RTPs of randomly selected slot machines
- Confirming the RTP from slot machines to Master Data: rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)
- Interviews & inquiries
- Identifying process weaknesses, risks and controls

Statement of Audit Standards

We conducted our audit 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.

Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Chances Kamloops, BCLC staffing component consists of a Manager Business Operations, one Senior Technician and one Technician. We noted during this audit that the BCLC staff at Chances Kamloops had a minimal staff turnover rate.

Conclusion

Audit Services found no RTP exceptions in the 99 machines tested on February 21, 2020 at Chances Kamloops.

Acknowledgements

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

Return to Player Settings Audit – Q4 Chances Salmon Arm

Audit Services

February 28, 2020

Table of Contents

Transmittal Letter 1

Introduction 2

Statement of Objectives 2

Statement of Scope 2

Statement of Methodology 2

Statement of Audit Standards 2

Personnel Changes in Key Control Areas 3

Conclusion 3

Acknowledgements 3

Transmittal Letter

March 23, 2020

Tom Maryschak
Senior Manager, Casino Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Mr. Maryschak:

Re: Return to Player (RTP) Audit –Chances Salmon Arm

Attached is the Audit Services' report on the RTP testing which occurred at Chances Salmon Arm Salmon Arm on February 28, 2020. The scope of our audit focused specifically on the RTP settings at Chances Salmon Arm for all slot machines.

During the course of our work conducted at Chances Salmon Arm, we noted that all 108 machines tested had their RTP settings set correctly. In total, Chances Salmon Arm has 108 slot machines.

We thank the management and staff of Chances Salmon Arm for their cooperation and assistance during this audit.

Sincerely,
s 22

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

cc: Kevin Sweeney, Director Security, Privacy and Compliance
Ken Bach, Regional Manager, Operations
Trevor Sharkey, Manager, Business Operations

Introduction

RTP Slot Management audit was included in Audit Services' approved audit plan for fiscal 2019-2020. These audits are to ensure the settings were set correctly based on information provided by the Casino and Community Gaming Product Team. RTP is the term the gaming industry uses to describe the percentage of all the wagered money a slot machine will pay back to players over time.

Statement of Objectives

Audit Services' objective through this engagement was to test the RTP settings at Chances Salmon Arm for the total populated for slot machines. The machines' current RTP settings were compared to the master data information looking for any discrepancies.

Statement of Scope

This audit is one component of several RTP audits scheduled to occur each fiscal quarter. The scope of these engagements includes the review of slot machine settings at various casinos and CGCs in the province for the period April 1, 2019 to March 31, 2020.

Statement of Methodology

Our methodology and approach included:

- Testing RTPs of randomly selected slot machines
- Confirming the RTP from slot machines to Master Data: rCasino database and/or Probability Accounting Reports (PAR) sheets (a PAR sheet details how a particular slot machine is programmed)
- Interviews & inquiries
- Identifying process weaknesses, risks and controls

Statement of Audit Standards

We conducted our audit 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.

Personnel Changes in Key Control Areas

BCLC's Audit Committee has requested that Audit Services include information about personnel changes and vacancies to key control areas during audit engagements. Personnel changes and vacancies can impact the control environment, control effectiveness, and loss of knowledge. At Chances Salmon Arm, BCLC staffing component consists of a Manager Business Operations, and one Senior Technician. We noted during this audit that the BCLC staff at Chances Salmon Arm had a minimal staff turnover rate.

Conclusion

Audit Services found no RTP exceptions in the 108 machines tested on February 28, 2020 at Chances Salmon Arm.

Acknowledgements

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

Vendor Security Controls Assessment – Salesforce

Audit Services

November 8, 2019

Table of Contents

Transmittal Letter 1

Introduction 2

Statement of Objectives 2

Statement of Scope 2

Statement of Methodology 2

Conclusion 2

Acknowledgements 3

Findings 3

1. Data Privacy Breach Response Planning and Documentation (moderate) 3
2. External Assurance Report Reviews (moderate) 4
3. External Assurance Report Distribution (moderate) 4

Appendix A – External Assurance Reporting 5

Appendix 2 – Technical Controls 5

Transmittal Letter

January 2, 2020

Pat Davis
CIO & VP, Business Technology
74 West Seymour
Kamloops, BC V2C 1E2

Dear Pat:

Re: Vendor Security Controls Assessment – Salesforce

Attached is the Audit Services' report on Vendor Security Controls Assessment on Salesforce.

Our findings herein include three recommendations that address two moderate and one low risk. Management has agreed with our recommendations and developed appropriate response plans to address each of the items identified.

We thank the management and staff of Business Technology for their cooperation and assistance during this audit.

Sincerely,

s 22

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

Introduction

As part of our fiscal 2019-2020 Annual Audit Plan, we are conducting Vendor Security Controls Assessments on third-party vendors who provide Software as a Service (SaaS) solutions to BCLC. This is an emerging cybersecurity risk area for all organizations that rely on SaaS solutions. BCLC relies on various SaaS vendors to provide core business functions and services as part of its operations. These solutions remotely store sensitive information that may include financial data, asset information, customer support documentation, player data and personally identifiable information. The purpose of this assessment was to review all external assurance reporting and the security controls that our vendors are applying to ensure the confidentiality, integrity and availability of BCLC's sensitive information.

Salesforce was selected for this review. Salesforce is utilized in BCLC divisions such as Marketing, Business Technology, eGaming, Lottery, and Customer Support Center. It provides a cloud-based online solution for customer relationship management (CRM) which allows a shared view of BCLC customers on one integrated CRM platform.

Statement of Objectives

As part of our assessment, we evaluated how Salesforce manages its information security risks by applying technical security controls and reviewing all relevant third-party assurance reporting against industry recognized standards and compliance. We determined whether the Salesforce application adopts information security best practices as relates to the confidentiality, integrity and availability of BCLC's sensitive information. Additionally, we determined whether BCLC has appropriate policy and procedures in reviewing relevant Salesforce assurance reporting.

Statement of Scope

Salesforce is an internal CRM application tool used by BCLC employees for Marketing, Business Technology, eGaming, Lottery and Customer Support Center. Sensitive information such as s 15(1)(l)

information is stored in this application in s 15(1)(l) on s 15(1)(l) data center. For this engagement, we assessed data from April 2019 to September 2019.

Statement of Methodology

The following procedures were conducted:

- Interviews with key personnel and questionnaires
- Review of procedures and practices
- Review of contracts, certifications and external assurance reports

Conclusion

Based on the assessment performed, we conclude that Salesforce applies appropriate technical controls, information security best practices and provides industry recognized external assurance reporting for its solution. Additionally, we identified improvement opportunities where management could enhance incident response planning and the sharing of assurance reports.

Acknowledgements

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

Findings

Following are the most significant issues that we identified during our work along with associated recommendations to address these issues. To assist management in prioritizing action plans in response to our recommendations, we have categorized each 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.
- Low – Issue is of lesser significance that is administrative in nature. Any low risk findings have been discussed with management and therefore excluded from the report.

These rating levels are measured in the context of this assessment and its objectives, rather than as related to overall corporate risk. Audit Services commits to conducting follow-up audits on all significant findings within six months from the date this audit report was issued.

1. DATA PRIVACY BREACH RESPONSE PLANNING AND DOCUMENTATION (MODERATE)

Finding

Lack of formally documented incident response plans for data privacy breaches and/or information security incidents specific to Salesforce.

Recommendation

In the event of a data privacy breach, management should have an incident response plan that is documented and tested periodically for Saleforce.com. The incident response plan should incorporate internal procedures with appropriate notification to internal/external stakeholders. The response plan should follow privacy breach protocols and guidelines from the Office of the Information Privacy Commissioner of British Columbia.

Management Response

Management agrees with this finding for Salesforce, as it does contain significant amounts of personal and confidential information. Management will partner with the BCLC Privacy team and Cyber Security team to develop a Salesforce specific incident response plan, in accordance with the guidelines and protocols of the Office of the Information Privacy Commissioner of British Columbia, as well as BCLC's existing Privacy Breach Policy. Management will perform a yearly test with these procedures to ensure they are effective and understood.

2. EXTERNAL ASSURANCE REPORT REVIEWS (MODERATE)

Finding

Management does not formally review external assurance reports provided by Salesforce.

Recommendation

Management should review external assurance reports regularly to track any significant findings for Salesforce. Any significant findings should be addressed in a timely manner to ensure that any risks to the confidentiality, integrity and availability of BCLC's sensitive information are mitigated.

Management Response

Management agrees with this finding. Management will establish a review cycle that aligns with the expiry schedule for each applicable assurance, in addition to a yearly review of all applicable assurances, for the Salesforce platform to identify and mitigate risks associated with changes to or failure to meet such assurances. The following applicable assurances will be monitored and reviewed:

- SOC 1
- SOC 2
- ISO 27001
- ISO 27017
- ISO 27018
- External Security Assessments (Vulnerability/Penetration)
- PCI DSS (as applicable, if credit card payments are implemented in Salesforce at BCLC)

3. EXTERNAL ASSURANCE REPORT DISTRIBUTION (MODERATE)

Finding

External assurance reports provided by Salesforce are not distributed to relevant internal stakeholders at BCLC.

Recommendation

Management should distribute assurance reports to relevant internal stakeholders to ensure business risks/impacts are understood, tracked and mitigated. These stakeholders may include Vendor Manager's, Cybersecurity, Privacy, Risk Advisory Services, and Business Continuity.

Management Response

Management agrees with this finding. Management will establish a list of pertinent stakeholders for each of the aforementioned assurances in order to respect the Salesforce Confidentiality Notice and Terms, as the assurances may contain confidential information and trade secrets.

At the scheduled review cycles, the pertinent reports will be made available to the established stakeholders for review and comment, in addition to being readily available anytime to authorize users on the Salesforce website (https://compliance.salesforce.com/en).

Appendix A – External Assurance Reporting

External Assurance Reporting	C5	HITRUST CSF Certified	ISO 27001 CERTIFIED	ISO 27017 CERTIFIED	ISO 27018 CERTIFIED	AICPA SOC	AICPA SOC	PCI DSS		
salesforce	Cloud Computing Compliance Controls	Risk Management & Compliance	Information Security: Business Centers	Information Security: Cloud Computing	Privacy Protection: Personal Information	SOC1 Type 2	SOC2 Type 2	Payment Card Industry Data Security Standards	Vulnerability Assessment	External Penetration Testing
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Appendix 2 – Technical Controls

Technical Controls	Data Host Location	Data Encryption	Single Sign-On	Vulnerability Patching	Incident Response	Backups	System Availability	Logical Access Controls	Physical Access Controls	Antivirus
salesforce	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	s 15(1)(l)			Yes	Priority Level/Response Times Defined	30 Day Retention Period	99.5%	Unique ID, Password Policy	Smart Card, Video Surveillance, Biometrics	All Servers and User Devices

ILC Audit of Effectiveness – Retailer Fraud & Customer Complaints

Audit Services

January 15, 2020

Table of Contents

Transmittal Letter 1
Introduction 2
Statement of Objectives 2
Statement of Scope 2
Statement of Methodology 2
Statement of Audit Standards 2
Audit Conclusions 3
Acknowledgements 3

Transmittal Letter

February 28, 2020

Craig James, Director Lottery Sales and Operations
Kevin deBruyckere, Director AML & Investigation
Sanam Bakhtiar, Director Lottery Marketing
Martin Lampman, Director Customer Support Operations
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear BCLC Management:

Re: ILC Audit of Effectiveness – Retailer Fraud & Customer Complaints

Attached is the Audit Services' report on the ILC Audit Effectiveness – Retailer Fraud & Customer Complaints.

As part of our FY2019-2020 approved audit plan, we completed the test of lottery controls effectiveness related to Retailer Fraud and Customer Complaints, specifically:

- Related Party or Associate Prize Claims
- ACL & Watchdog Reports
- Integrity and Security Related Incidents or Complaints
- Retailer GPEB Registration (coordinated with GPEB)
- Mystery Shop Failures and Remedies

Based on our audit we noted that overall lottery control on Retailer Fraud and Customer Complaints are working as expected. Any improvement areas noted have been shared with management.

We thank the management and staff of Player Services, Customer Support Operations, Security Investigations and Lottery Sales for their cooperation and assistance during this review.

Sincerely,
s 22

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

cc: Kevin Gass, VP Lottery Gaming

Introduction

Audit Services conducts a Lottery compliance audit against the Interprovincial Lottery Corporation (ILC) Standards on an annual basis. In 2011, the ILC requirement for audit testing changed from a test of effectiveness to a test of design only. However, Audit Services continued to perform test of effectiveness on specific ILC Standard areas to provide additional assurance on BCLC lottery control environment.

For FY2019-2020, Audit Services completed the effectiveness test on ILC Standard 12D, Retailer Fraud and ILC Standard 12I, Customer Complaints.

Statement of Objectives

The objective of this engagement was to assess the effectiveness of the Lottery Control Environment, specifically on Retailer Fraud and Customer Complaints.

Statement of Scope

The scope of this engagement includes:

- Related Party Prize Claims
- Audit Command Language (ACL) & Watchdog Reports
- Integrity/Security Related Incidents/Complaints
- Retailer GPEB Registration (will rely on GPEB's Audit)
- Mystery Shop Failures and Remedies

Statement of Methodology

Audit Services performed sample testing of the following:

- Related party claims and documentation
- ACL & Watchdog reports
- Integrity/security related incidents
- Review GPEB's audit working paper on retailer registration
- Mystery Shop failures & remedies

Statement of Audit Standards

We conducted our audit 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.

Audit Conclusions

Based on our audit, we noted that existing Lottery Controls over Retailer Fraud and Customer Complaints are effective. Audit Services will continue to test lottery control effectiveness on other ILC Standards in an annual basis.

Acknowledgements

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

Access Controls

Personally Identifiable Information Systems – SuccessFactors

Audit Services

March 19, 2020

Table of Contents

Transmittal Letter 1

Introduction 2

Statement of Objectives 2

Statement of Scope 2

Statement of Methodology 2

Conclusions 2

Acknowledgements 2

Assessment Findings 3

1. Disabling s 15(1)(l) Access (Moderate) 3
2. s 15(1)(l) Access Reviews (Moderate) 3

Transmittal Letter

March 24, 2020

Sarah Turtle
Senior Manager, HR Strategic Projects
74 West Seymour
Kamloops, BC V2C 1E2

Dear Sarah:

Re: Access Controls PII Systems – SuccessFactors

Attached is the Audit Services' report on Access Controls – PII (Personally Identifiable Information) – SuccessFactors.

Our findings herein include two recommendations that address two moderate risk topics. Management has agreed with our recommendations and developed appropriate response plans to address each of the items identified.

We thank the management and staff of People and Culture for their cooperation and assistance during this engagement.

Sincerely,

s 22

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

cc: John Leeburn, VP, People and Culture

Introduction

The SuccessFactors system is used by internal BCLC staff for several core human resource functions. It contains several modules for recognition (badges), recruitment, performance management and training. Sensitive information such as s 15(1)(l) is stored in this application. The purpose of this audit was to assess the access controls for the SuccessFactors system to ensure that necessary access controls are being applied to maintain confidentiality, integrity and protection of sensitive information.

Statement of Objectives

The objectives of this engagement were to:

- Determine if management has access controls in place to manage user access to the in-scope system, and to determine if those controls are working effectively.
- Assess the SuccessFactors system's access controls as it relates to sensitive information.

Statement of Scope

The scope of this engagement included a review of management practices as relates to access controls for the SuccessFactors system. The scope included all users of the SuccessFactors system across BCLC's corporate offices during Q3 of FY2020.

Statement of Methodology

The following procedures were conducted:

- Interviews with key personnel and questionnaires
- Review of procedures and practices
- Documentation review

Conclusions

Based on the work performed, we conclude that management's technical controls can be further strengthened for the SuccessFactors system. Information security best practices around access controls must be applied to ensure access is authorized, modified and revoked in a timely manner. Audit Services commits to conducting a follow-up on all significant findings within in Q2 of FY2021.

Acknowledgements

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

Assessment Findings

Following are the most significant issues that we identified during our work along with associated recommendations to address these issues. To assist management in prioritizing action plans in response to our recommendations, we have categorized each 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.
- Low – Issue is of lesser significance that is administrative in nature. Any low risk findings have been discussed with management and therefore excluded from the report.

These rating levels are measured in the context of this assessment and its objectives, rather than as related to overall corporate risk.

1. DISABLING s 15(1)(l) ACCESS (MODERATE)

Finding

s 15(1)(l) have active accounts in the SuccessFactors system. No documentation or process exists for managing s 15(1)(l) accounts.

Recommendation

s 15(1)(l) to mitigate any unauthorized access. A process for enabling and disabling s 15(1)(l) accounts should be developed as a guideline to manage s 15(1)(l) access to SuccessFactors.

Management Response

Management agrees with this finding. A process change will be made to ensure s 15(1)(l) BCLC will remove or suspend s 15(1)(l) access to the system. Regular reviews of s 15(1)(l) access will occur on a quarterly basis.

2. s 15(1)(l) ACCESS REVIEWS (MODERATE)

Finding

No documented s 15(1)(l) access reviews have been completed for the SuccessFactors system. s 15(1)(l) have elevated privileges, which includes the ability to for change configurations and assign permissions.

Recommendation

s 15(1)(l) access reviews should be completed to ensure that s 15(1)(l) access is appropriate and revoked in a timely manner to prevent unauthorized configuration changes and access to sensitive data. s 15(1)(l) access reviews should be conducted regularly. Management should also review and remove inactive s 15(1)(l) accounts over a predefined period.

Management Response

Management agrees with this finding. This group is closely monitored and without management approval no one can be added to this listing. HRMS team has added a quarterly review of the list to our mandatory system release process.