



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

VIA EMAIL

February 14, 2020

[applicant information]

Re: Request for Records: BCLC File 20-001

British Columbia Lottery Corporation (BCLC) writes further to your January 2, 2020 request (received on January 3, 2020) under B.C.'s *Freedom of Information and Protection of Privacy Act* (FIPPA) and BCLC's letter dated January 9, 2020.

You requested:

"[1] Full texts of all audits from your internal audit branch, from April 8, 2019, until [January 2, 2020]. Also send a list of plan of all areas and topics due to be audited."

Based on similar requests clarified with you quarterly since July 1, 2017, BCLC interpreted your current request in a similar manner to be for:

"[1] Full texts of all audits from your internal audit branch, from April 8, 2019, until [January 2, 2020]. A list of areas and topics due to be audited in the current fiscal year [April 1, 2019 to March 31, 2020]."

BCLC has been proactively disclosing internal audit reports on the "Reports and Disclosures" page of bclc.com on a quarterly basis since August 4, 2017. As a result, some of the information you have requested is publicly available on BCLC's Reports and Disclosures website under the heading for "Accountability."

Internal audit reports for the timeframe of April 1, 2019 to June 30, 2019 (FY 2019-20 Q1) are located here:

https://corporate.bclc.com/who-we-are/corporate-reports/corporate-reports-search.html?filter_category=accountability

Internal audit reports for the timeframe of July 1, 2019 to September 30, 2019 (FY 2019-20 Q2) and for October 1, 2019 to December 31, 2019 (FY 2019-20 Q3) are being excepted from disclosure under section 20(1)(b) of FIPPA that states:

"The head of a public body may refuse to disclose to an applicant information... (b) that, within 60 days after the applicant's request is received, is to be published or released to the public...."

We will notify you of the release of the information on or before March 30, 2020, as required under section 20.

The full text of section 20 can be found at:

http://www.bclaws.ca/Recon/document/ID/freeside/96165_00

Internal audit reports for the timeframe of January 1, 2020 to March 31, 2020 (FY 2019-20 Q4) have not yet been completed. However, there was one internal audit completed during the timeframe of your request from January 1, 2020 to January 2, 2020 that falls within FY 2019-20 Q4. This audit will not be published within the required timeframe set out under section 20 of FIPPA. As a result, BCLC is providing one record (seven pages) with some information withheld under sections 15 and 22 of FIPPA. Below are the reasons for withholding information under each of the exceptions to disclosure noted.

Section 15 (harm to computer systems)

The information withheld under this section could harm the security of a system, including BCLC's computer and communication systems, under section 15(1)(l) of FIPPA.

Section 22 (harm to personal privacy)

The information withheld under this section consists of the signature of a BCLC employee. Disclosure of this information would be an unreasonable invasion of personal privacy because it could result in identity fraud.

In accordance with section 6(2) of FIPPA, BCLC has created a record (one page), enclosed, in response to the portion of your request for:

“a list of areas and topics due to be audited in the current fiscal year [April 1, 2019 to March 31, 2020].”

BCLC notes that you routinely make a request under FIPPA for information that is publicly available. In these cases, BCLC will not open a file. Before submitting an FOI request, please refer to bclc.com to see if the information you seek has been published.

This response will be published a minimum of five business days after release at:
<https://corporate.bclc.com/who-we-are/corporate-reports/reports-disclosures.html>

If you have any questions or concerns regarding BCLC's processing of your request, please contact me via e-mail at clantos@bclc.com or at (250) 377-2076.

Additionally, under section 52 of FIPPA, you may ask the Information and Privacy Commissioner to review this reply to your request for information. You have 30 business days from the receipt of this notice to request a review by writing to:

Office of the Information and Privacy Commissioner for British Columbia
P.O. Box 9038, Station Provincial Government
Victoria, BC V8W 9A4
T (250) 387-5629 F (250) 387-1696
Email info@oipc.bc.ca Online www.oipc.bc.ca

Sincerely,
[original signed by]

Candice Lantos
Senior Freedom of Information Analyst

Enclosure

Audit Services FY2019-2020 Remaining Planned Audits

The list below summarizes the planned audit activities for Audit Services for the remainder of the 2019-2020 fiscal year. This list was developed using a transparent, risk-based audit planning approach by working with BCLC's board, executive and management. The design of our plan is to remain flexible and responsive to change, whether changes come from emerging risks, new projects or changes to the organization's controls. Ultimately, this will allow Audit Services to deliver the greatest value to our stakeholder while efficiently managing internal resources.

This list is a snapshot of the projected audit activities for the remainder of the 2019-2020 fiscal year. It is important to note that this list may be subject to change based on emerging risks, new projects, organization control changes and resourcing requirements.

List of Planned Audits

- Cybersecurity Incident Response
 - ILC Control Standards
 - Lottery Controls Framework ILC Test of Effectiveness
 - Vulnerability Management
 - Access Reviews
 - Casino Return to Player (RTP) Management:
 - GameSense Locational Testing
 - Host Local Government Payments
 - IT General Controls (supporting KPMG)
 - Holdback (Pensionable Portion)
 - HR Policy and Procedures
-

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 § 15(1)(l)

information is stored in this application in § 15(1)(l) on § 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 Salesforce.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										
	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
	✓ Eastern Canada AWS Data Center	✓ 256-bit	✓ TLS 1.2	✓ 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