Department of Justice and Attorney-General

Office of Liquor and Gaming Regulation

Cloud Computing Regulatory Framework

Version 1

Queensland Government

For further information, please contact the Office of Liquor and Gaming Regulation on 13 QGOV (13 74 68) or visit https://www.business.qld.gov.au/industry/liquor-gaming

Contents

1 Objective

This document sets out the regulatory approach determined by the Office of Liquor and Gaming Regulation (OLGR) in relation to the assessment of 'cloud computing' for use within the Queensland liquor and gambling industry.

It sets out some of the minimum considerations to be applied by the OLGR when assessing and monitoring cloud computing arrangements, and does not impede or replace any existing legislative or regulatory requirements regarding such arrangements and/or associations entered by licensees.

This document does not override any other requirements or standards that the licensee must comply with when utilising cloud technology.

2 Scope

This document includes information that is required to ensure regulatory oversight can be maintained by the OLGR. The document also includes mandatory information required for formal approvals pursuant to the *Lotteries Act 1997*, the *Wagering Act 1998*, the *Keno Act 1996*, the *Gaming Machine Act 1991*, the *Casino Control Act 1982* and the *Liquor Act 1992*, when licensees propose to use cloud computing for regulated systems, data or records.

3 Regulated gaming equipment

3.1 What is cloud?

The Australian Government Cloud Computing Policy (2014) defines cloud computing as '…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction…'

3.2 Variations of cloud

Cloud computing arrangements include the following service models.

3.2.1 Software as a service

The 'Software as a Service' model is the ability to use the cloud provider's applications running on a cloud infrastructure. An example of this is web-based email. The provider controls and maintains the physical computer hardware, operating systems and software applications. The customer only controls and maintains limited application configuration settings specific to users, such as email address distribution lists.

3.2.2 Platform as a service

The 'Platform as a Service' model is the ability to deploy onto the cloud infrastructure customer-created applications. The customer does not manage or control the underlying cloud infrastructure (including hardware, operating systems and storage media), but has control over the deployed applications. The cloud provider provides the infrastructure plus operating systems and server applications, such as web servers. The cloud provider controls and maintains the physical computer hardware, operating systems and server applications. The customer only controls and maintains the software applications developed by the customer.

3.2.3 Infrastructure as a service

The 'Infrastructure as a Service' model is the ability to store computing resources where the customer is able to deploy and run software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, applications and possibly networking components, such as host firewalls. The cloud provider may or may not provide the physical computer hardware (including CPU processing, memory, data storage and network connectivity) and may share amongst multiple 'tenants' using virtualisation software. This enables customers to run operating systems and software applications (and possibly hardware) of their choice.

4 Key regulatory considerations

4.1 Applications for use of cloud technology

4.1.1 Types of applications

As the use of cloud technology will involve a variation to several existing approvals that exist in relation to the operation of gaming by licensees in Queensland, the licensee must be cognisant of the impact of cloud and be transparent in its application to the OLGR.
Use of cloud technology may include, but not limited to, a submission of an application for the OLGR to approve:

- places of operation
- places of storage of records
- changes to the network policy
- changes to the gaming system(s) to facilitate cloud
- changes to the data storage / operation location(s)
- other systems that achieve regulatory objectives
- any other required submissions.

4.1.2 Content of applications for the use of cloud

Type of cloud intended to be used

Applications should stipulate the way in which the selected service model will be deployed. This may include but not limited to:

- private cloud—provisioned for exclusive use by a single organisation comprising multiple users (e.g. business units). It may be owned, managed and operated by the organisation, a third party or some combination of them, and may exist on or off premises
- community cloud—provisioned for exclusive use by a specific community of consumers that have shared concerns. It may be owned, managed and operated by one or more of the organisations in the community, and may exist on or off premises. An example of this is the sharing of a private cloud by several agencies of the same government
- public cloud—provisioned for open use by the general public. It may be owned, managed and operated by a business or government organisation, and exists on the premises of the cloud provider. This model has maximum potential cost efficiencies; however, it has a variety of inherent risks that need to be considered. It means reduced costs, but also increased potential security concerns
- hybrid cloud—a composition of two or more of the above distinct cloud models that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability.

Specifics in relation to the entity that will provide the cloud solution to the licensee

Applications should include details of the service level agreements between the licensee and the cloud provider.

Service level agreements should clearly identify ownership of data and control of data. They should also identify the physical and legal location of the provider, and the jurisdiction in which the agreement is enforced, including how disputes will be resolved.

Typically applications will be reviewed against a risk profile. Higher risk applications are those that propose to conduct or operate core gaming systems via the cloud, or otherwise are used to store or provide services that can affect the integrity of a gaming system or a game.

Higher risk applications would typically be required to include a high-level system architecture design document and a security document that assesses how the integrity of the products and services are maintained, including how systems are deployed, verifiable, auditable and remain available where relevant.

Licensee risk assessment of the entity and the cloud solution

All applications should be accompanied by a formal risk assessment that includes the tools used to make the assessment. The risk assessment should address technical risks, business operational risks, financial risks, legal and regulatory compliance risks, and information management risks. Information management risks include:

- sensitive information will be leaked
- information cannot be retrieved from the provider, and will be lost.

The risk assessment should address any possible weakening of current security arrangements as a result of the implementation of cloud arrangements.

Evidence should be provided that the use of cloud computing complies with legislation, standards, policies and licence conditions.

4.1.3 Key OLGR considerations when determining applications in relation to cloud technology

Is the intended supplier of cloud to the gaming licensee a reputable organisation?

Some reliance may be placed on the provider's professional certifications. The licensee should consider which are relevant and how much the certification increases overall confidence. Associated documents should be evaluated by the licensee and provided. For example, for providers citing ISO/IEC 27001 compliance, the Statement of Applicability, a copy of the latest external auditor's report, and the results of any internal audits should be reviewed by the licensee and made available.

An evaluation of the provider's guarantee of the availability and quality of service should be conducted, including software version control and change management processes, if applicable. In addition, the guarantee of availability should include scheduled outages.

Assurance should be sought to ensure timely provider support, and maximum acceptable response times should be identified in service level agreements that support any licensee obligations to the government (e.g. in standards and licence conditions).

Are contractual arrangements with cloud service provider adequate?

No matter which service model or deployment model is selected, the contract between a provider and a licensee must address mitigations to governance and security risks that arise from deploying systems, records or data in a cloud environment. This should include who has access to the licensee's data, and the security measures used to protect the data.

All security related considerations must be captured in the service level agreement with the cloud provider.

Record security controls

Assurance should be obtained that the provider is capable of, and will execute, complete destruction of deleted records and prevent unauthorised disposal.

The OLGR should be notified of all security incidents, preferably via secure communication. If there is a security breach, such as unauthorised access to data, the extent to which the provider will provide investigatory assistance should be detailed. Access to audit logs should be made available.

Contingency plans should be in place to facilitate portability and interoperability to easily move to a different provider should the current provider be no longer available.

With regard to multi-tenancy arrangements (where physical hardware such as memory drives is shared by multiple tenants), assurance needs to be given that virtualisation mechanisms (the techniques used to partition shared resources between tenants) guarantee adequate logical segregation between multiple tenants.

Secondary storage facility

Consideration should be given to keeping a secondary backup of business-critical data, state-government-vital data and personal/sensitive data to address the risk of loss of data. If an up-to-date copy of the data is to be stored with a second provider, it should be ensured that there are no common points of failure with the first provider.

Data restoration capacity

The adequacy of partial or full restoration of data should be considered, including the maximum acceptable time.

If a second provider is to be used for business continuity or disaster recovery, it should be ensured that the replication be configured to transition automatically and smoothly, and this should be tested in accordance with any requirements in the relevant OLGR technical standards.

Suitability of network connectivity

Network connectivity to the cloud should be assessed for adequacy in terms of availability, traffic throughput (bandwidth), delays (latency) and packet loss. Also, data encryption technologies should be evaluated to ensure protection while data is in transit. Gateway technologies such as firewalls and anti-virus software should be considered. Assurance needs to be obtained that the provider has no access to passwords or data encryption keys.

Location of data

All cloud services should be guaranteed to remain within Australia. This obligation is in addition to any obligations that exist in legislation, licence conditions or standards, some of which require systems and data to remain either within Australia or within Queensland.

The OLGR must be supplied with exact details of how the device performs the hash over its software/firmware.

4.2 Post-approval regulatory considerations

It is expected that an established set of controls and monitoring be developed to ensure that the cloud provider and the cloud-based service continues to be fit for purpose and sufficiently

robust to protect the integrity of gaming in the State.

As a result, the OLGR will require all licensees to advise of the following, which may trigger, especially for higher risk implementations, a requirement for further review and approval.

- changes to the way the cloud service is provided which may have a material effect on the way the OLGR regulates the licensee and the products or services within, including potential effects on the integrity of gaming
- changes in the cloud provider itself or service or other agreements
- concerns arising about the cloud provider's accreditation
- changes to the data storage location, including secondary storage
- changes to the operational location
- changes to security controls.

5 References

Australian Government Information Management Office, *Australian Government Cloud Computing Policy*, Version 2.0 May 2013, Department of Finance and Deregulation <https://www.finance.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf>

Department of Science, Information Technology and Innovation, *Queensland Government Cloud Computing Strategy*, May 2014, Department of Science, Information Technology and Innovation, Brisbane <https://www.qgcio.qld.gov.au/__data/assets/pdf_file/0014/4712/170280-cc-strategy-v2.pdf>

Victorian Commission for Gambling and Liquor Regulation 2019, *Regulatory Approach to Cloud within the Victorian Gambling Industry,* Victorian Commission for Gambling and Liquor Regulation, Melbourne.

6 Useful links

https://www.qgcio.qld.gov.au/ict-strategy/cloud-computing
https://en.wikipedia.org/wiki/Data_sovereignty

7 Revision history

Version	Changes	QIR	Who	Release date	Incept date
1.0	Initial Release		Ops	21/10/2019	21/10/2019
Incept notes:					