ALDERNEY GAMBLING CONTROL COMMISSION

Standards and Guidelines for eGambling Cloud

Version 2.6.1

December 2019

Document Revision History

Version	Date	Change detail	Changed	Authorised
0.1	August 2013	First AGCC Draft	NH	
0.2	August 2013	Second AGCC Draft – Discussion Draft	NH	MGE
1.0	November 2013	First public release	NH	JS
1.1	April 2016	Minor language changes	NH	TF
2.5	July 2018	Expanded the introduction, simplified and clarified some sections, added the Cloud Risk Assessment	NH	NB
2.6	June 2019	Clarified Hosting Certificate references	NH	
2.6.1	December 2019	Fixed broken links in table 1	NH	

Standards and Guidelines for eGambling Cloud

AGCC approach to Cloud use for regulated activity

Introduction

AGCC has adopted the following position on cloud use for regulated activity:
"Use of an external publicly available cloud, provided from outside the AGCC approval process, may be used for simple web servers, displaying informative web pages, landing pages, resource delivery etc. However, where any part of regulated *game play, financial or registration process where personal, financial, or game transaction information may be handled within those external systems*, such activities must be performed only where it is considered by AGCC to be safe and secure under Regulation 205(b).
For such an operation to be considered safe and secure, the cloud provider will have to comply with, and may have gained approval against, the standards documented in AGCC published "Standards and Guidelines for eGambling Cloud" (this document).

These Standards contemplate Cloud use in four categories:

Private Cloud
The cloud infrastructure is provisioned for exclusive use by a single licensee potentially comprising multiple consumers (e.g., business units of that licensee). It may be owned, managed, and operated by the licensee, a third party, or some combination of them.

Community Cloud
Community cloud infrastructure involves a private cloud that is owned and operated by an AGCC approved person, that is shared by several licensees, or suitable entities, with similar security requirements and a need to store or process data of similar sensitivity. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud. An example community cloud is the sharing of a vendor private cloud by several licensees.

Public Cloud
The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them.
This form of deployment is subject to approval against these AGCC guidelines and standards.

Hybrid Cloud
The cloud infrastructure is a composition of the two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
This form of deployment is subject to approval against these AGCC guidelines and standards.
The detailed proposals for the standards follow.

The above systems may be provided and deployed in various ways, including, but not limited to:

Infrastructure as a service (IAAS), where the cloud provider supplies what may appear to be "bare metal" servers to the licensee, upon which the licensee deploys it's Internet Gambling architecture or,

Platform as a service (PAAS), where the cloud provider supplies virtual servers already set up with the fundamental operating systems etc. for the licensee to build its systems upon, or

Software as a service (SAAS), where the Cloud provider supplies some form of ready to run applications already installed and deployed for the licensee,

Audience
The requirements in this document are aimed mainly at the intending Gambling cloud system providers (**GCP**). Where it is aimed at the AGCC licensee will be noted in the text, and highlighted in **bold** where appropriate. It is expected that AGCC licensees will have completed a Cloud Risk Assessment **(CRA)** relating to cloud deployment, an example of which is appended to this document as Appendix A.

Executive Summary
As the use of the term "Cloud Computing" is interpreted differently by a myriad of organisations, it is important to take note of the AGCC definitions of "Cloud" in Section 1 below.

Boiled down, obtaining approval for providing gambling services or producing and storing sensitive data in the Cloud involves the following simple steps:

1) The *cloud provider* may obtain a "Hosting Certificate" (essentially a prudential check of the business) from the AGCC.
2) The *cloud provider* must produce a static "package" of all relevant ISO and other formal Certifications, relevant to the building, deployment and operation of the IAAS/SAAS etc. systems that they wish to provide to the AGCC licensee. This may also include some parts of their approved ISMS under ISO 27001 pursuant to this document. This package should be delivered to the licensee, or to the AGCC if a Hosting Certificate application has been made.
3) The AGCC will evaluate the package and make a decision to approve or otherwise, the proposed eGambling Cloud systems.
4) The **AGCC licensee** may then deploy and activate an Internet Gambling System in the approved infrastructure. This must be correctly documented in the **licensee's ICS**. Note that some details around security in Section 5 may need to be provided to the licensee by the eGambling *cloud provider*.

SECTION 1: Preliminary

Introduction

The Alderney Gambling Control Commission (AGCC) recognises that cloud computing systems provide many commercial advantages to eGambling systems and licensees. Similarly such systems provide benefits to the AGCC as a regulatory authority (in particular the "availability" attribute of security).

However, cloud computing systems also bring commercial and regulatory risk (particularly to the "integrity", "confidentiality" attributes of security, and "jurisdictional" considerations). As with all eGambling systems operating pursuant to the Alderney eGambling Ordinance, eGambling in cloud computing systems requires AGCC approval.

Audience

This document is provided for both licensees and intending *Gambling Cloud System Providers* (GCP). In many cases this document will have particular relevance to GCP vendors.

Purpose & objective

The purpose of this document is to:

a. provide guidelines and requirements guiding licensees and cloud systems service providers with a road map to achieve approval of cloud systems for use in the eGambling industry, regulated by AGCC;

b. ensure risks to regulatory and jurisdictional policies and objectives are controlled and managed where cloud systems are used for eGambling;

c. provide a basis for non-gambling industry best-practice framework utilisation in the eGambling sector.

Scope & applicability

These guidelines and standards relate to cloud systems which are not provided by a Category 2 Licence or Certificate holder under the Alderney regulations.

These guidelines and standards relate to eGambling cloud systems':

a. security management systems requirements,

b. security management systems certification requirements, and

c. submission for approval of GCP requirements

and are within the scope of this document.

This document compliments the AGGC's Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems document.

eGambling functionality must be certified pursuant to the AGCC *Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems*, Alderney Regulations and Ordinance, however, cloud systems may be certified to broader industry standards as described herein.

Out-of-scope

This document does not provide guidance on all matters likely to be considered by the AGCC in relation to GCP. Matters such as probity of licensee associates and GCP's are not addressed by this document.

Limitations

These guidelines and requirements are published at a time when many national and international standards are yet to be published.

AGCC definitions of cloud systems

1.1.1 Deployment models

1.1.1.1 Private cloud

The cloud infrastructure is provisioned for exclusive use by a single licensee potentially comprising multiple consumers (e.g., business units of that licensee). It may be owned, managed, and operated by the licensee, a third party, or some combination of them.

1.1.1.2 Community cloud

Community cloud infrastructure involves a private cloud that is owned and operated by an AGCC approved person, that is shared by several licensees, or suitable entities, with similar security requirements and a need to store or process data of similar sensitivity. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud. An example community cloud is the sharing of a vendor private cloud by several licensees.

1.1.1.3 Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them.

This form of deployment is subject to approval against these AGCC guidelines and standards.

1.1.1.4 Hybrid cloud

The cloud infrastructure is a composition of the two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

This form of deployment is subject to approval against these AGCC guidelines and standards.

1.1.2 Service models

1.1.2.1 Software as a service (SaaS)

The capability provided to a licensee is to use a vendor's applications running on cloud infrastructure. The applications may be accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The licensee does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited licensee-specific application configuration settings (e.g. pay-table on slot machines).

1.1.2.2 Platform as a service (PaaS)

The capability provided to the licensee is to deploy onto the cloud infrastructure licensee-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The licensee does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

1.1.2.3 Infrastructure as a service (IaaS)

The capability provided to the licensee is to provision processing, storage, networks, and other fundamental computing resources where the licensee is able to deploy and run arbitrary software, which can include operating systems and eGambling or related applications. The licensee does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

1.1.3 eGambling assets at increased risk through cloud systems

eGambling functionality is any functionality that would normally be regulated by AGCC under Alderney Ordinance, Regulations or described in the *Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems*.

Licensees, vendors, and GCPs must have integrated information security management systems which include all eGambling activities "in-scope". The AGCC has a low tolerance to risk to eGambling operated pursuant to the Ordinance. This section outlines the AGCC position with regard to inherent risk resulting from the use of cloud systems. The relevance of ISO/IEC 27001 recommended controls is shown in the table on page 21.

1.1.3.1 Jurisdictional

The AGCC considers there is extreme heightened jurisdictional and legal inherent risk where eGambling functions are placed under the control of cloud systems.

1.1.3.2 Confidentiality

The AGCC considers the confidentiality of customer personal, gaming, and financial data may be placed at heightened inherent risk where eGambling functions are placed under the control of cloud systems.

The AGCC also considers the confidentiality of in-play gaming data is at heightened inherent risk where eGambling functions are placed under the control of cloud systems. *Guidance: "confidentiality" of in-play gaming data, such as cards dealt in poker affects the "integrity" of the game.*

1.1.3.3 Integrity

The AGCC considers the integrity of transaction logs and gaming functionality is at heightened inherent risk where eGambling functions are placed under the control of cloud systems.

1.1.3.4 Availability

The AGCC considers the availability of gaming and financial transaction logs and customer accounts may be at heightened inherent risk where eGambling functions are placed under the control of cloud systems.

SECTION 2: REQUIREMENTS

Overview

It is the AGCC's objective in establishing these guidelines & requirements that industry best-practice may be utilised in the certification of cloud systems for eGambling. Consequently, **licensees** and associated GCP may either have cloud related information security management systems certified to ISO/IEC 27001 or have the systems certified by another entity which meets the criteria established in this document.

The AGCC draws on *ISO/IEC 27001 Information technology – Security techniques - Information security management systems – Requirements* [***Ref D***] as an authoritative basis to the AGCC approach. This approach is outlined in ISO/IEC 27001 clause 0.2 [***Ref D***]. Note that for purposes of this document however, ISO/IEC 27001 clause 0.2 b) [***Ref D***] should be amended to read, "***implementing and operating controls to manage an organisation's information security risks in the context of the organisation's overall business risks in particular regulatory risks to Guernsey, Alderney, and the Alderney Gambling Control Commission***".

eGambling functionality must be approved, and compliant to the AGCC *Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems* [***Ref B***] however, cloud systems may be certified to broader industry standards as described herein.

Information security management system

Cloud computing which touches eGambling functionality or data should be operated pursuant to an *information security management system* (ISMS) [***Ref D***].

Licensees and GCP may be guided by ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management in implementing ISMSs [**Ref E**].

2.1.1 Scope

All personnel, products, and processes which may affect the safety, security, fairness, or legal status of eGambling cloud computing should be included in the ISMS scope, refer ISO 27001 clause 4.2.1 a) [***Ref D***].

Boundaries may often be defined by clarifying personnel, products, or processes which are out-of-scope. That is, where a business specifically defines components that are out-of-scope, then the components in-scope may be more apparent.

2.1.2 Contractual requirement to comply

Licensees should ensure all contracts with all business partners and GCP mandate a requirement for those entities to comply with the requirements set-out in this document, refer ISO/IEC 27001 clause 4.2.1 b) 2) "contractual security obligations" [***Ref D***].

To facilitate efficient compliance assurance of this requirement licensees should maintain a complete register of contracts, refer ISO/IEC 27001 clause 4.3.3 [***Ref D***].

2.1.3 Geographic location

The GCP should include a concise list of the premises and the geographic location (legal jurisdiction) of all sites where infrastructure may be used in the cloud system which affects eGambling functionality or data. NOTE: where the risk assessment determines the geographic location of all sites is highly sensitive and requires strong controls relating to confidentiality, then the concise list may be provided directly to the AGCC.

Where an eGambling system operates in jurisdictions other than Alderney or Guernsey then the ISMS should include continuous monitoring of the legal status of operations within all relevant jurisdictions and ensure continuous legality (ISO/IEC 27001 clause 4.2.3 d) 6) [***Ref D***]).

NOTE: the AGCC may require the applicant to provide evidence in the form of written legal opinion as to the legal status of the proposed eGambling cloud computing system for each relevant jurisdiction.

2.1.4 Risk management

The ISMS should be supported by a risk management programme.

Licensees and GCP may use *IEC/ISO 31010:2009 Risk management – Risk assessment techniques* [***Ref H***] as an appropriate process.

For each legal entity with a stake in the ISMS there should be Board approval of the risk management plan and acceptance of the residual risk within that plan.

Evidence of satisfactory adherence to the above processes should be available to the AGCC.

Licensees and GCP are guided that the purpose of this document is to satisfy the objectives of the AGCC including the satisfactory management of regulatory and jurisdictional risk. Thus in addition to the references in this section the following sub-sections also apply.

AGCC Licensees should have completed a Cloud Risk Assessment (CRA), an example of which is set out in Appendix A.

2.1.4.1 Establishing the context

Licensees and GCP are advised that the regulatory and jurisdictional risk threshold is most likely to be low in contrast to commercial entities, context considerations should be consistent with regulatory & jurisdictional risks and objectives.

The criteria for accepting risk should be documented and available to the AGCC, refer ISO/IEC 27001 clause 5.1 f) [***Ref D***] and IEC/ISO 31010 clause 4.3.3 c) and d) [***Ref H***].

2.1.4.2 Risk assessment

Licensees and GCP are advised that the regulatory and jurisdictional risk threshold is most likely to be low in contrast to commercial entities, risk assessments should be consistent with regulatory & jurisdictional risks and objectives.

There should be a Risk Assessment Report encapsulating the activities described in this section, refer ISO/IEC 27001 4.2.1 c) to g) [***Ref D***].

2.1.4.3 Risk treatment

Licensees and GCP are advised that the regulatory and jurisdictional risk threshold is most likely to be low in contrast to commercial entities, risk treatments should be consistent with regulatory & jurisdictional risks and objectives.

All risks that are transferred to other parties (see ISO/IEC 27001 clause 4.2.1 f) 4) [***Ref D***] should be compiled in a register or specifically flagged such that the AGCC may readily identify the risks transferred by the licensee and/or GCP to third parties.

2.1.5 Statement of applicability

The licensee and/or GCP should maintain a contemporaneous statement of applicability as set out in ISO/IEC 27001 4.2.2 j) [***Ref D***].

The statement of applicability should be approved by the Board of the licensee.

2.1.6 Implementation & operation ISMS

Licensees and/or GCP are referred to ISO 27001 clause 4.2.2 [***Ref D***] as an expectation as to the minimum components of the ISMS.

Licensees and/or GCP are referred to ISO 17799 (ISO/IEC, 2005) for implementation guidance.

Monitoring and review

At least annually licensees and GCP should provide evidence of monitoring and review. Monitoring should be contemporaneous and incorporate changes to the scope, people, processes, or products covered by the ISMS.

Monitoring and review should include all laws in all relevant jurisdictions, see ***2.1.3 Geographic location*** on page 12.

Continuous improvement

Licensees and GCP should ensure ISMS are continuously improved. For the purpose of ISO/IEC 27001 clause 4.2.4 [***Ref D***] "regularly" should be monthly and should be not less than biannual.

For the purposes of ISO/IEC 27001 clause 4.2.4 c) [***Ref D***] "interested parties" should include the AGCC.

Control of ISMS & operational documents & records

All documents and records, including iterations of dynamic registers, should be maintained in a manner that the integrity and availability of the documents and records is maintained, refer ISO/IEC 27001 clauses 4.3.2 and 4.3.3 [***Ref D***].

The control of documents should be within the scope of the ISMS and statement of applicability.

All transactions and records that touch an AGCC eGambling record of a customer of a **licensee** associated with the AGCC should be securely retained for 5 years after the last transaction of that customer.

All documents and records encompassed by this document should be available to the AGCC and the Guernsey Financial Services Commission for 5 years after the last transaction of any customer to whom those documents or records may relate through the life of transactions of that customer. This requirement should be integral to the scope of the ISMS, refer *THE PREVENTION OF MONEY LAUNDERING AND COMBATING THE FUNDING OF TERRORISM (AGCC2013)*.

Certification of information security management system

The ISMS should be certified.

ISMSs may be certified against ISO/IEC 27001 [***Ref D***] by an organisation itself accredited to *ISO/IEC 17021:2011 Conformity assessment - Requirements for bodies providing audit and certification of management systems* [***Ref C***] or by an organisation specifically recognised by the AGCC.

SECTION 3: Approval process

This section describes the process for seeking AGCC approval of a cloud system.

Cloud systems ISMS conformance certification

Cloud systems should be operated pursuant to an ISMS which is certified to be in conformance with ISO/IEC 27001 [***Ref D***]. In accordance with the SECTION 2: REQUIREMENTS ISMS

Submission material

The submission should be made up of:

a) Copies (not links) of certifications to the various standards discussed above that have been issued by a Certified entity (*table1* can be used as a guide),

b) For any part that has not been covered by an ISO type certification, a documented procedure that is used as a compensating control by the applicant.

Documentation	Reference(s)	
3.1.1 ISMS scope	ISO/IEC 27001 4.2.1 a)	2.1.1 Scope
3.1.2 Register – geographic locations	ISO/IEC 27001 4.2.1 a)	2.1.3 Geographic location
3.1.3 Register - contracts	ISO/IEC 27001 4.3.3	2.1.2 Contractual requirement to comply
3.1.4 Risk management methodology	ISO/IEC 27001 4.2.1 c) IEC/ISO 31010 4.3.3 c)	2.1.4.1 Establishing the context
3.1.5 Risk assessment report	ISO/IEC 27001 4.2.1 c), d), e), f),and g)	2.1.4.2 Risk assessment
3.1.6 Risk treatment plan	ISO/IEC 27001 4.2.2 b)	2.1.4.3 Risk treatment
3.1.7 Basis of control exclusions	ISO/IEC 27001 4.2.2 g) and 4.2.2 j) 3)	2.1.4.3 Risk treatment
3.1.8 Consolidated list of transferred risk	ISO/IEC 27001 4.2.1 f) 4)	2.1.4.3 Risk treatment
3.1.9 Documentation supporting the effectiveness of controls	ISO/IEC 27001 4.2.3 c)	Monitoring and review
3.1.10 Evidence of Board of licensee acceptance of risk	ISO/IEC 27001 4.2.1 h) ISO/IEC 27005 9.3	Residual risk
3.1.11 Statement of applicability	ISO/IEC 27001 4.2.1 j)	2.1.5 Statement of applicability
3.1.12 Evidence of ISMS compliance (certificate and report)		Certification of information security management system
3.1.13 Evidence of certifier accreditation		Certification of information security management system

Table 1 – guide to what is expected to be covered in a submission for approval of eGambling cloud computer system

GCP process

3.1.14 Description of process

3.1.14.1 Confirming certification complies with AGCC requirements

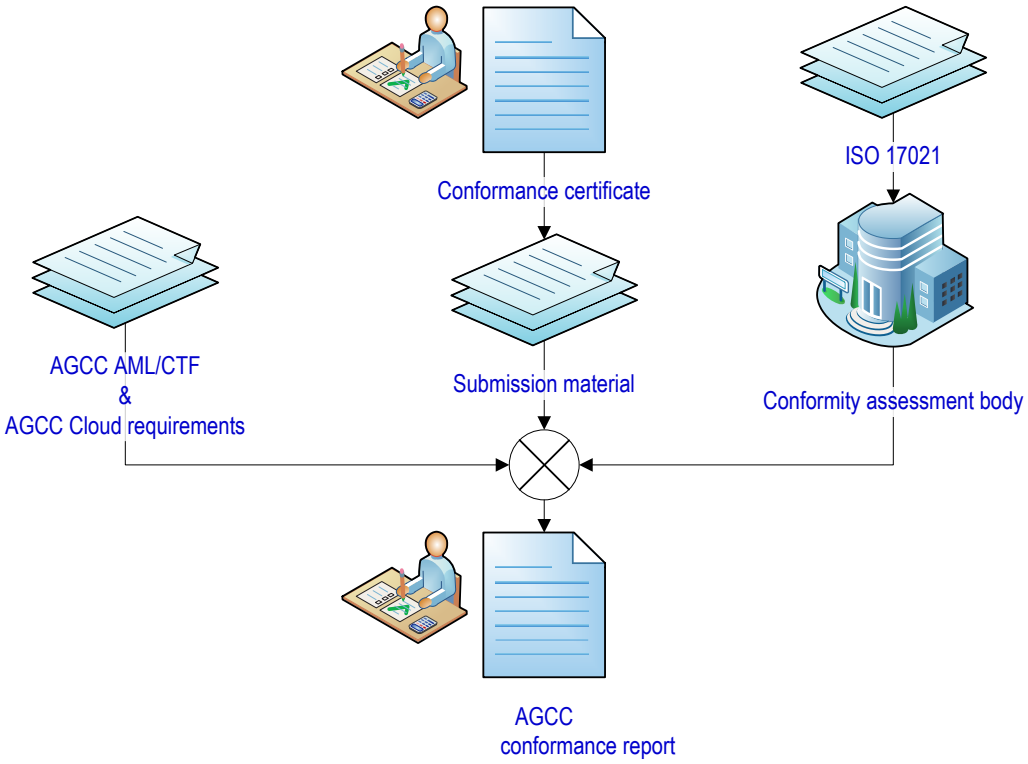

Figure 1 - AGCC conformance validation

The AGCC will accept the submission material as described above, and will assess the suitability of the eGambling Cloud offering. The assessment may lead to further questions. ***It is likely that a visit by officers of the AGCC or its agents to one or all of the hosting sites to support the assent will be required.***

Conformance at this stage is indicative that the GCP services may be acceptable for eGambling (subject to AGCC approval).

eGambling certification

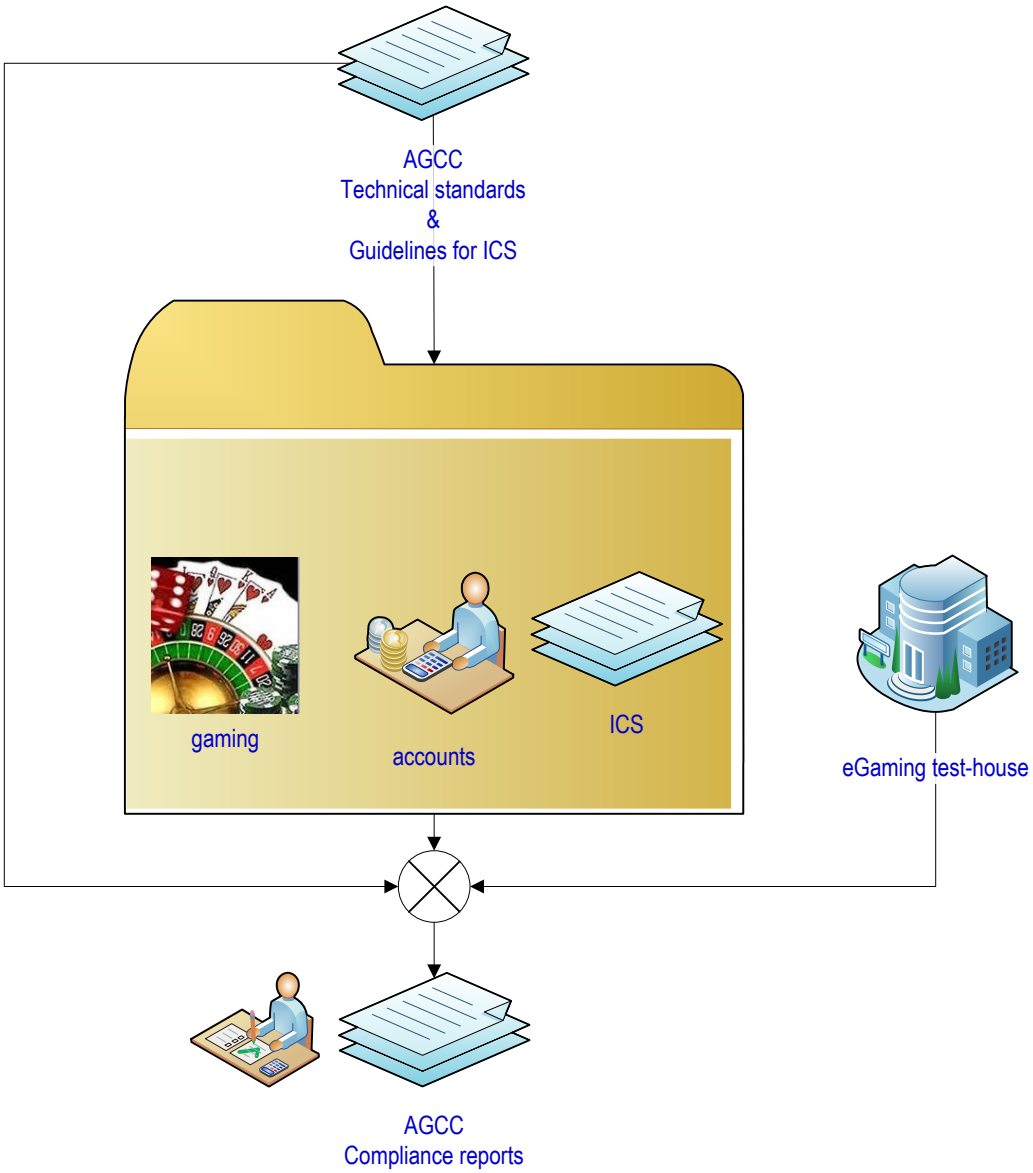

Figure 2 - abstract of eGambling certification process

The existing eGambling certification process for eGambling functionality remains unchanged. Where it is proposed aspects of the standards or guidelines should be incorporated under GCP approval then these should be clearly identified in the *AGCC compliance reports* issued by the *eGambling test-house*, refer ***Figure 2 - abstract of eGambling certification process***.

AGCC GCP approval and deployment

Among the AGCC considerations are the proposed eGambling on the GCP implementation model. The AGCC must be satisfied the full scope of matters have been considered in the eGambling certification (outlined in section

eGambling certification).

Deployment models of GCP may vary between implementations. ***Figure 3 - eGambling components deployed in GCP system*** shows a conceptual implementation with the eGambling activities of *accounts* and *gaming* deployed to aGCP.

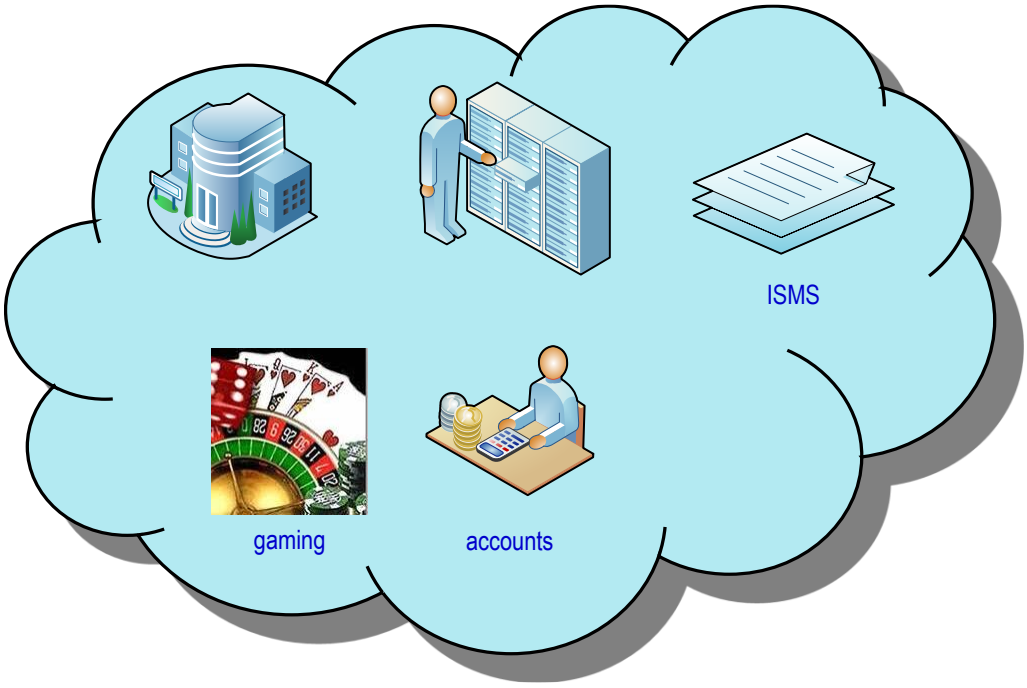

Figure 3 - eGambling components deployed in GCP system

Critical eGambling components

This section categorises eGambling components such that where these activities are a component of an information processing system then that information processing system should be the subject of an information security management system. For the purpose of these guidelines these eGambling components are critical eGambling components. Examples of critical eGambling components are pseudo-random number generators, while examples of non-critical eGambling components are information servers.

Critical eGambling components include:

- Random Number Generators (RNG's)
- Gaming servers
- Gaming Databases
- Client Database which contain sensitive information
- Jackpot Servers
- Any system which creates an outcome of a gambling transaction
- Sportsbook or betting exchange servers
- Registration servers (where a client enters personal identifiable information to register to play for "real" money)
- "Hot" standby systems
- Administration servers used to control the gaming systems

Risk management

All controls listed at ISO/IEC 27001 Annexe A [***Ref D***] are considered relevant for the use of cloud systems for GCP. This Annexure provides guidance as to the AGCC's inherent view of the relevance of the controls set out in ISO/IEC 27001 AnnexeA [***Ref D***].

The controls in ISO27001 Annexe A are rated by AGCC approximation of relevance (0-9) against the regulatory and jurisdictional objectives of "C" confidentiality, "I" integrity, "A" availability, and "J" jurisdictional sovereignty - 9 being most relevant.

The higher a control is ranked here, then the higher the onus on the justification where controls are excluded in the risk treatment (see ***2.1.4.3 Risk treatment***).

ISO 27001	relevance (0-9)				
Annexe A	C	I	A	J	Additional comments
A.5.1.1	8	8	7	7	
A.5.1.2	8	8	7	7	
A.6.1.1	8	7	6	7	
A.6.1.2	7	7	7	7	
A.6.1.3	7	7	7	7	
A.6.1.4	7	7	7	7	
A.6.1.5	6	6	6	6	
A.6.1.6	5	5	5	5	
A.6.1.7	4	4	4	4	

ISO 27001	relevance (0-9)				
Annexe A	C	I	A	J	Additional comments
A.6.1.8	8	8	8	7	Annually
A.6.2.1	8	8	8	5	Includes corporate cloud users.
A.6.2.2	8	8	8	8	
A.6.2.3	8	8	8	7	NB It's noted that this might exclude information access for legitimate regulatory and legal compliance.
A.7.1.1	5	5	5	8	
A.7.1.2	7	6	6	8	
A.7.1.3	7	7	7	6	
A.7.2.1	7	7	7	8	All critical eGambling information and information processing should be limited to jurisdictions where the eGambling activity is legal.
A.7.2.2	6	5	5	6	
A.8.1.1	7	7	7	5	
A.8.1.2	7	7	7	7	If the GCP infrastructure is accessible by employees from a jurisdiction where privacy restricts background checks then this is "high risk" and must be considered in the remedial controls.
A.8.1.3	7	7	7	7	
A.8.2.1	7	7	7	5	
A.8.2.2	7	7	7	5	
A.8.2.3	7	7	7	8	If the GCP employees are in a jurisdiction which limits disciplinary actions, then this must be addressed in the risk programme.
A.8.3.1	7	7	7	7	
A.8.3.2	7	7	7	7	
A.8.3.3	9	9	9	6	
A.9.1.1	8	8	8	8	
A.9.1.2	8	8	8	8	
A.9.1.3	8	8	8	8	
A.9.1.4	8	8	8	8	
A.9.1.5	9	9	9	8	
A.9.1.6	8	8	8	8	
A.9.2.1	8	8	8		
A.9.2.2	8	8	8		
A.9.2.3	8	8	8	8	
A.9.2.4	8	9	8		

ISO 27001	relevance (0-9)				
Annexe A	C	I	A	J	Additional comments
A.9.2.5	8	8	8	8	
A.9.2.6	9	5	5		
A.9.2.7	9	5	8		
A.10.1.1	8	8	8	8	Documented procedures should be available to the AGCC or its agents (on request).
A.10.1.2	9	9	9	9	
A.10.1.3	8	8	8		
A.10.1.4	9	9	7		
A.10.2.1	8	8	9	9	
A.10.2.2	8	8	9	9	
A.10.2.3	9	9	9	9	
A.10.3.1	7	7	9	9	
A.10.3.2	8	8	9	9	
A.10.4.1	9	9	7		
A.10.4.2	9	9	7		
A.10.5.1	9	9	9	8	
A.10.6.1	9	9	9	8	
A.10.6.2	9	7	9		
A.10.7.1	9	5	6		
A.10.7.2	9	5	5		
A.10.7.3	9	5	7		
A.10.7.4	9	9	7		
A.10.8.1	8	6	7		
A.10.8.2	8	6	7		
A.10.8.3	9	5	7		
A.10.8.4	9	8	5		
A.10.8.5	8	5	5		
A.10.9.1	9	8	6		
A.10.9.2	9	9	9		

ISO 27001	relevance (0-9)				
Annexe A	C	I	A	J	Additional comments
A.10.9.3	9	7	7		
A.10.10.1	8	6	6		
A.10.10.2	8	6	7		
A.10.10.3	9	7	8		
A.10.10.4	9	8	8		
A.10.10.5	7	7	9		
A.10.10.6	7	8	7		
A.11.1.1	8	6	7		
A.11.2.1	8	6	6		
A.11.2.2	9	6	7		
A.11.2.3	8	6	7		
A.11.2.4	8	6	7		
A.11.3.1	8	6	7		
A.11.3.2	8	6	7		
A.11.3.3	6	6	6		
A.11.4.1	8	8	8		
A.11.4.2	8	7	7		
A.11.4.3	6	8	6		
A.11.4.4	9	9	8		
A.11.4.5	9	8	7		
A.11.4.6	9	6	6		
A.11.4.7	8	8	7		
A.11.5.1	8	8	8		
A.11.5.2	8	6	7		
A.11.5.3	9	6	7		
A.11.5.4	9	9	8		
A.11.5.5	8	5	5		
A.11.5.6	6	7	6		

ISO 27001	relevance (0-9)				
Annexe A	C	I	A	J	Additional comments
A.11.6.1	9	9	7		
A.11.6.2	8	9	8		Critical eGambling components should have heightened controls.
A.11.7.1	8	6	6		
A.11.7.2	8	5	5		
A.12.1.1	9	9	9		
A.12.2.1	5	8	8		It is recognised this is principally a licensee implemented control and not a GCP implemented control.
A.12.2.2	9	9	9		This is particularly critical for poker (i.e. hole cards confidentiality and fairness of subsequent cards drawn).
A.12.2.3	5	8	8		
A.12.2.4	8	8	8		
A.12.3.1	8	5	8		
A.12.3.2	8	5	8		
A.12.4.1	9	9	9		
A.12.4.2	5	5	5		
A.12.4.3	7	8	5		
A.12.5.1	7	7	7		
A.12.5.2	7	7	7		
A.12.5.3	9	9	9		
A.12.5.4	9	5	5		
A.12.5.5	6	6	6		
A.12.6.1	7	7	7		
A.13.1.1	8	8	8		The AGCC should be routinely notified at the earliest time.
A.13.1.2	8	7	7		
A.13.2.1	8	7	7		
A.13.2.2	8	7	7		
A.13.2.3	8	8	8	8	GCPs should ensure all logs and evidence are collected in a means suitable for prosecution in each jurisdiction that the cloud spans, including but not limited to Alderney and Guernsey.
A.14.1.1	7	6	9	7	Regardless of the BCP and restoration jurisdiction all data relating to a licensees business pursuant to the Ordinance should remain available to the AGCC.
A.14.1.2	6	6	9	7	
A.14.1.3	6	6	9	7	

ISO 27001	relevance (0-9)				
Annexe A	**C**	**I**	**A**	**J**	**Additional comments**
A.14.1.4	6	6	9	7	
A.14.1.5	6	6	9	7	
A.15.1.1	9	7	9	9	
A.15.1.2	7	7	7	9	
A.15.1.3	8	7	9	9	
A.15.1.4	9	7	9	9	Cross border privacy laws - written legal opinion relating to the compliance with EU Privacy laws and laws of each relevant jurisdiction.
A.15.1.5	7	8	7	8	
A.15.1.6	8	5	9	9	
A.15.2.1	9	9	9	9	
A.15.2.2	9	9	9	9	Annually
A.15.3.1	7	7	9		AGCC or agents should be granted unfettered access regardless of jurisdiction.
A.15.3.2	8	6	7		

Glossary

In this document the definitions set out below apply.

Term	Meaning	Reference
asset	anything that has value to the organisation, the Alderney Gambling Control Commission, Alderney, or Guernsey.	Derived from ISO/IEC27000
availability	property of being accessible and usable upon demand by an authorised entity.	ISO/IEC27000
confidentiality	property that information is not made available or disclosed to unauthorised individuals, entities, or processes.	ISO/IEC27000
integrity	property of protecting the accuracy and completeness of assets.	ISO/IEC27000
security	preservation of confidentiality, integrity, and availability of information and information processing systems.	derived from ISO/IEC27000
should	the text relates to a guideline or requirement	
system	an integrated composite of people, products, and processes that provide a capability to satisfy the stated needs or objectives.	MIL-HDBK-520A

Synopsis of relevance of documents referenced

This document describes requirements and a methodology which utilise standards applicable to non-gambling specific standards. This section provides an overview and summary of the relevance of documents cited in this guidance and requirement.

These references are dynamic. Emerging international standards and best-practice documents will necessitate frequent reviews of this document. It is the responsibility of the reader to ensure the version relied upon is up-to-date.

AGCC AML/CFT

Org'	Title	Date
AGCC	THE PREVENTION OF MONEY LAUNDERING AND COMBATING THE FUNDING OF TERRORISM	2013

Ref A

The AML/CFT guidance for the Alderney eGambling industry based in Alderney. These guidelines are based on the Financial Action Task Force (FATF) "40 + 9 recommendations".

AML/CFT documents establish data availability (maintenance duration) period.

AGCC standards & guidelines

Org'	Title	Date
AGCC	Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems	25-04-2013

Ref B

Technical standards and control systems guidelines, particularly those relating to gambling functionality and data confidentiality and availability remain relevant whether the eGambling system is in a stand-alone homogeneous eGambling platform or GCP's system(s).

ISO/IEC 17021

Org'	Title	Date
ISO/IEC	Conformity assessment - Requirements for bodies providing audit and certification of management systems Conformity assessment -- Requirements for bodies providing audit and certification of management systems - Part 2: Competence requirements for auditing and certification of environmental management systems Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 3: Competence requirements for auditing and certification of quality management systems	01-02-2011

Ref C

ISO/IEC 17021 contains principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types and for bodies providing these activities. Certification of management systems is a third-party conformity assessment activity. Bodies performing this activity are therefore third-party conformity assessment bodies.

Conformity assessment bodies ensure appropriate certification of the ISMS and/or the scope and boundaries of any such certification in the context of the requirements established within this document.

ISO/IEC 27001

Org'	Title	Date
ISO/IEC	Information technology – Security techniques - Information security management systems - Requirements	15-10-2005

Ref D

ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organisations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.

This standard is central to the AGCC approach outlined in this document. Where cloud computing systems are not specifically approved by the AGCC then the AGCC requires compliance with ISO 27001 or equivalent standard. Furthermore, this document provides guidance as to risk thresholds and control selection necessary to meet the AGCC requirements.

ISO/IEC 27002

Org'	Title	Date
ISO/IEC	Information technology - Security techniques - Code of practice for information security management	15-06-2005

Ref E

ISO/IEC 27002 provides implementation guidance for best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS).

ISO/IEC 27005

Org'	Title	Date
ISO/IEC	Information technology – Security techniques - Information security risk management	01-06-2011

Ref F

ISO/IEC 27005 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. It does not specify or recommend any specific risk analysis method. It does however, specify a structured, systematic and rigorous process from analysing risks to creating the risk treatment plan.

ISO/IEC 27017 (information)

Org'	Title	Date
ISO/IEC	Information technology - Security techniques - Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Draft

Ref G

ISO/IEC 27017 will likely have a very direct impact on these AGCC guidelines and requirements. At time of writing the standard is in final draft and included here as a guide as to likely future amendments.

ISO 31000

Org'	Title	Date
ISO	Risk management – Principles and guidelines	15-11-2009

Ref H

The purpose of ISO 31000 is to provide principles and generic guidelines on risk management. ISO 31000 seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes to replace historic standards, methodologies, and paradigms that differed between industries, subject matters, and regions.

Because of the inherently prescriptive nature of eGambling requirements GCP are required to include the regulatory and jurisdictional assets and risk thresholds of the AGCC and jurisdiction.

IEC/ISO 31010

Org'	Title	Date
IEC/ISO	Risk management – Risk assessment techniques	11-2009

Ref I

The ISO 31010 standard supports the ISO 31000 standard. It supplies a guide as to the selection and application of risk assessment techniques.

Risk management is a requirement and a cornerstone of the methodology required by this document. The precise risk management technique is not mandated but this international standard is provided as guidance.

Because of the inherently prescriptive nature of eGambling requirements GCP are required to include the regulatory and jurisdictional assets and risk thresholds of the AGCC and jurisdiction.

APPENDIX A: Example Cloud Risk Assessment (CRA)

Risk	Description	Impact	Type of risk Regulatory or Reputational	Mitigation	Fully Mitigated
Overall infrastructure risk	Licensee not in full control of hardware and data security	High	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence • Approval of the eGambling Cloud system by the AGCC	
Loss of player identifiable data	Player information in the cloud may be either stored unsafely or "cloned" by the cloud owner Or accessed by a third party such as a contractor.	High	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence • Encrypt all sensitive data. • Install robust security processes.	
Loss of commercial data, including Game Play	Proprietary software and commercial data may be stolen or cloned by hackers or accidently accessed by a third party.	Med	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. Contractual confidence Install robust security processes Isolate commercial data on secured servers.	
Unauthorised access to IGS	The servers (virtual and physical) that make up the IGS may be accessed & therefore compromised by unauthorised actors.	High	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence • Monitor and control all access to IGS	
Unauthorised access via privileged user profiles, such as the administration Portal	The administration systems (where games etc. are configured) that make up the IGS may be accessed & therefore compromised by unauthorised actors	High	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. • Due Diligence on the operators of the games and how they deal with staff etc • Contractual confidence • Remove standard privileged accounts provided. • Lock configuration files and monitor them. • Ensure all privilege user profiles are maintained in-house.	
Changing of DNS configuration	The DNS is how players, operators and other users "find" the gaming systems on the Internet. If this is changed, people may actually be going to a "fake" or cloned system	Med	Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence • Secondary DNS under a different hosting arrangement as a failsafe Monitor DNS closely	
Cloning of IGS	The owner of the cloud IAAS can simply clone the entire system and make a working copy.	HIGH	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider. • Regulatory approval of the hosting provider	

				• Due Diligence on the provider and how they deal with staff etc. • Contractual confidence • Approval of the eGambling Cloud system by the AGCC	
Jurisdiction of gambling transactions	If the IAAS/ cloud supplier have a fully extensible system across Jurisdictions, then we must ensure that gambling transactions do not occur in any Jurisdiction that is not approved.	Med	Reg/Rep	• Best if the Cloud provider has a hosting certificate from the AGCC • Approval of the eGambling Cloud system by the AGCC • Ensure that the Cloud provider is 100% aware of the risks and contracts to keep Virtual servers in agreed Jurisdictions.	
Unauthorised access to data at rest	Information that is in the database, or any data stored at call can be accessed by the cloud provider, and possibly hackers	High	Reg/Rep	• Full encryption of the data at rest • Ensuring the cloud provider does NOT have access to the encryption keys • Proper ISO certified private key handling processes	
Lack of hosting certificate	If the owner of the hosting holds a "hosting Certificate", then the licensee need not be concerned with collecting ISO certificates etc. prior to approval.	Med	Reg	• Best if the Cloud provider has a hosting certificate from the AGCC • Approval of the eGambling Cloud system by the AGCC	
Man in the Middle ("MITM") attack on games, financial transactions	The owner of the cloud system can sit between the games server or financial server and the player and monitor the traffic, thus gaining sensitive data. This risk exists with privately hosted systems but the added threat in Cloud environments is many parties including service employees can position themselves in the middle.	Med	Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider • Due Diligence on the provider and how they deal with staff etc • Contractual confidence	
MITM attack on API to Licensees (B2B)	The owner of the cloud system and (potentially) hackers can sit between the games server and a serviced B2P Casino system and monitor the traffic, thus gaining sensitive data.	Low	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence	
Location of private keys	Private encryption keys can be extracted from the terminating server and stolen (to be used to impersonate the site, at the very least) by the Cloud provider	Med	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence • Ensure only Private keys that NEED to be installed on servers are installed, and ensure that the systems are in place to alert of tampering or to destroy the keys on extraction.	
Firewall configuration safety	Firewalls provided a virtual machines as IAAS can be copied and thus their configuration known by the Cloud provider, and potentially hackers that	High	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence	

	have access to the providers systems			• Avoid “software” application level firewalls and ensure that there are physical firewalls at the perimeter	
Network diagrams	If the actual network diagrams are stored with the same cloud provider or the diagrams can be generated there, then the system can potentially be compromised.	Low	Rep	• Contractual confidence • Ensure that the data on navigating the network is not in the same place as the network	
Security of Operating system and patching	Depending upon the type of Cloud service provided (bare metal or OS installed) The OS patching and building is a critical security point	High	Reg/Rep	• Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence • Use local staff to harden and install OS • Patch ONLY for known sources • Ensure patching is kept up to date.	
Source code in the cloud	If any source code is kept on Cloud servers, the owner of the cloud system and other potential “Bad Actors” could copy it or examine it for vulnerabilities etc.	high	Reg/Rep	• Ensure end to end encryption • Ensure that local staff create the repository • Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence	
Fault reporting in the cloud	Listings of faults or problem ticketing systems , for example Jira, in the Cloud could lead to the weaknesses of the systems being known by bad actors	high	Reg/Rep	• Ensure that local staff create the repository • Full ISO27001 certification (and others) of operation of the systems by the provider. • Due Diligence on the provider and how they deal with staff etc. • Contractual confidence	
Loss of technical “know how” in the business	If the Cloud provider offers SAAS , where complete systems like firewalls etc. are provided complete, there the understanding of how the network works, and how to protect it may erode over time	Med	Rep	Ensure staff are kept up to date on the technical sides of the systems	