Guidelines | Technical Infrastructure hosting Gaming and Control Systems

Remote Gaming

December 2015

Table of Contents

1. Introduction

1.1. Background

Network infrastructure topologies vary considerably among online gaming operators, with operators often opting to locate their servers in jurisdictions other than the one in which the remote gaming operator is licensed. The infrastructure in use can be owned or outsourced (or indeed a hybrid of both) creating different control and oversight requirements with respect to the proper governance of an online gaming operation. In recent years this matter has been made more complex and challenging with the advent of cloud solutions. Either as a stand-alone solution, or in combination with traditional co-location and managed services solutions, cloud solutions offer a multitude of advantages for the operator.
From gaming operators' perspective, the network topology - including the location of servers - is often an issue of cost, distance or rather proximity from markets served, operators' or their providers' technology and operational resources, reliability, quality and a host of other factors. Together these compel operators to locate their system data in one jurisdiction or another or a combination of solutions that suit particular operators and their regulatory, operational and technological situation.

The importance of ensuring adequate supervision over an operator's gaming and control systems lies at the core of the Malta Gaming Authority's (MGA) regulatory functions, with the final objective being the safeguarding of player and regulatory interests by providing an environment with the required level of security and data integrity. Specifically, from a regulatory perspective, it is important for the MGA to have timely access to all the regulatory data in order to ensure that it remains well-positioned to conduct its supervisory functions, at pre- and post- licensing stages, that include the possibility of carrying out regular inspections, auditing and, or *ad hoc* investigations.

The MGA recognises that the technical infrastructure located in Malta allows for timely audits and investigations and this has assisted in operators' checks in support of improved compliance performance. Over time, this situation has grown and evolved as it adapted to technological developments, as well as to operators' increasingly multi-jurisdictional operations. These, in turn, have resulted in an array of network configurations which required revisiting the approaches to compliance-monitoring in order to ensure that operators can maximise on technological developments, including those from cloud solutions, while continuing to ensure the required rigour in compliance.

1.2. Purpose

The purpose of these guidelines is to underline and update the MGA's approach when implementing its regulatory requirements and procedures with respect to Technical Infrastructure. They are intended to guide operators, other providers, and stakeholders on the Authority's compliance objectives and what is taken into consideration when evaluating an applicant's, or a licensee's technical set-up. These guidelines will be kept under review and will be updated as necessary from time to time.

1.3. Approach

The MGA recognises that, in attaining its regulatory objectives and in ensuring its continued ability to conduct its supervisory functions, it needs to take cognisance of an evolving and diverse situation. This requires a more principles-based approach (rather than a set of prescriptive rules) that takes into consideration a risk evaluation. The MGA's acceptance and approval of a particular proposal will largely depend on the treatment of risks posed by any one particular proposal.

In the adoption and implementation of the principles-based approach, these guidelines should be complemented with an open, frank and constructive dialogue between the applicants/licensees, and the MGA. The applicants'/licensees' willingness to mitigate risks and reach the compliance targets and regulatory outcomes will be key.

Such an approach has the intended effect of allowing the operators to exploit the benefits of technology, including cloud solutions, without jeopardising the Authority's regulatory interest and regulatory outcomes, which remain paramount.
The principles-based approach is being complemented by the identification of accepted industry standards that the MGA considers to meet its compliance requirements. The acceptance and approval of a particular proposal will be largely dependent on an assessment of the risks posed. In view of this, and subject to mitigation measures that are adopted, deviations from these standards will also be considered.

1.4. Applicability of principles and guidelines

The principles set out in this paper are already embedded in the MGA's internal regulatory policies and administrative practices routinely employed in assessing remote gaming licence applications and ongoing compliance. They shall therefore continue to apply to all remote gaming licensees and applicants.

Although the obligations derived from being a remote gaming licence holder do not apply directly to service providers of co-location and cloud services, the MGA urges these providers to be guided by the standards referred to in these guidelines.

2. High-level principles and Regulatory objectives

2.1. General principles

Proportionality: the MGA seeks to adopt and implement control mechanisms and procedures that are proportionate to the risk posed by any operator/situation, namely that the application of these guidelines and requirements by the MGA shall be proportionate to the risk posed by the technical infrastructure / configuration presented by the operator.

Consistency of outcomes: the MGA is seeking the same level of regulatory performance, and therefore regulatory outcomes, by the operators. Consistency of outcomes requires a steadfast pursuit to meet the set compliance performance targets, irrespective of the technical infrastructure, processes and/or systems that are employed.

Suitability: the principles-based approach objectively seeks to allow for a level of adaptability in how the regulatory objectives and outcomes can be met within the set principles.

2.2. Specific regulatory objectives

The actual physical technical infrastructure and its location has been, and will remain, important as a means of ensuring that regulatory data, and the infrastructure on which it is hosted, is safe, secure and accessible at all times for compliance, consumer protection and business continuity purposes.

The MGA considers that the location of the technical infrastructure is critical for the attainment of the highest level of regulatory principles that are more readily applicable to the actual data, its hosting and processing, including:

Integrity and security: the integrity of regulatory data, including transaction logs and gaming functionality, must be ensured at all times.

Availability, traceability and accessibility for regulatory compliance purposes: gaming and financial transaction logs must be accessible at all times. In this area, and with data being hosted on servers and in data centres outside Malta, including cloud environments, there may be an issue of jurisdiction of same data that may affect accessibility by the MGA for regulatory purposes.

Privacy and confidentiality: this refers particularly to personal, gaming and financial data that must comply with data protection rules.

Accountability: the responsibility for the attainment of the established and desired standards on these regulatory principles will remain that of the licensee at all times.

3. Implementation and conformity with objectives

3.1 Integrity and security

Hosting architecture - General guidance

Licensees/applicants are required to provide details of the technical Infrastructure, including a network schematic, showing all the hardware and virtual machines in operation with the respective internal IP addresses, including all the geographic locations and addresses of premises where the technical infrastructure hosting gaming systems, control systems and regulatory data[1] will be located.

In instances where the licensee/applicant wishes to maintain systems in a cloud environment, a complete list of all geographic locations and addresses of premises where the infrastructure may or shall be used should be submitted to the Authority at the time of application.

The Authority, in assessing a proposal or application and establishing its position, will take into consideration the geographic location of the critical components (see below) of the operation. **The architecture must be located in Malta, and/or any EEA member state and/or in any other third country jurisdiction wherein the Authority is satisfied that the same principles can be obtained.** Such assessments, in particular, those concerning locations in third party jurisdictions, will be conducted on a case-by-case basis.

Data Security at hosting locations, including cloud environments

The MGA requires that hosting locations wherein licensees/applicants locate their technical infrastructure should conform to a high level of information security and should be subject to an Information Security Management System (ISMS) throughout the term of a gaming licence[2].

The information security level the MGA seeks is that of ISO/IEC 27001:2013 and CSPs (Cloud Service Provider) are to be guided by ISO/IEC 27002:2013 Information

[1] Regulatory data comprises player details, financial transactions and game-play transactions
[2] For the avoidance of any doubt, this shall include the term during which a licence may be suspended.

Technology - Security techniques - Code of Practice, for Information Security Management in implementing the Information Security Management System.

Apart from the ISO standards mentioned above, and specifically with respect to credit card or other payment data storage or processing of information, the Authority shall seek PCI DSS Level 1 certification. The PCI Security Standards Council is considered by the MGA to offer robust and comprehensive enough standards and supporting materials to enhance payment card data security.

Hosting locations that are certified as per the above standards will facilitate the processing of an application, provided that applicants may be required to provide proof of such certification.

Critical Components

Some components (including processes) of an operator's system/s are considered as 'critical'. The MGA considers a component or components as being 'critical', when there is increased regulatory and/or business integrity, safety, privacy and compliance risk. The MGA considers the following to be critical components:

- Random Number Generators (RNGs);
- Jackpot servers;
- Player database servers;
- Financial database servers;
- Gaming database servers; and
- Any other component deemed by the MGA to be critical within the system organisation of the operator.

Hosting of critical components on cloud systems

Any decision by operators to utilise a cloud environment for the hosting of all or part of their critical components should follow the conducting of a risk assessment within the framework and process of risk management described in the ISO 31000:2009. The risk assessment should include the core elements of the risk management process as defined in this standard.

The submission of the operators risk assessment, primarily with respect to the risks listed in Appendix A and how they will be managed and mitigated, will form the basis of the MGA's review.

The risks listed in Appendix A have been identified with a view to ensuring the attainment of the principles listed in section 2 above. These risks focus mainly on the adoption and use of cloud environments and highlight the fact that operators might face additional risks (similar to those found within the traditional environment). This list should therefore not be considered an exhaustive list of risks and operators should carry out the assessment based on their operational set-up.

The MGA considers that further conditions should apply due to the additional risks that a cloud environment may pose.

The Authority will be satisfied that the proposed architecture meets the principles contained in these guidelines when the critical components are hosted on a private cloud environment which is not shared with other tenants on the same cloud.

Virtual private cloud environments will be allowed when the Authority is satisfied that the integrity and security of the critical components is not at risk.

3.2 Availability, traceability and accessibility

Availability, traceability and accessibility of licensee's regulatory data[3] for supervision purposes are key for the MGA. In order for the Authority to carry out its regulatory function it requires access to real time information.

Access to live information becomes even more difficult when the licensee's infrastructure is located in other jurisdictions and, or cloud environments.

This limitation can be overcome through the provision of a real time replication of regulatory data, on a live replication server in Malta.

MGA's assessment concerning replication of data in Malta

Any application proposal submitted to the Authority should include the following:

a. Details about the replicated server including physical location, rack number and IP addresses;
b. Details about the connectivity to the live servers, including details of the security protocols in place for the transmission of data;
c. Details on the type of data being replicated and its transmission frequency including time lags, if any, between the processes taking place on the live servers and the replication servers. This should provide adequate assurances of real time replication, security, confidentiality and integrity of data.
d. A fully-documented procedure, allowing MGA officials immediate and unhindered access to be able to conduct routine or *ad hoc* inspections on the replication server, (both physically and electronically) as may be required.

The MGA reserves the right to amend the data set that must be replicated on the basis of the risk profile of the proposed system and/or business model, or location of live infrastructure.

[3] Regulatory data is composed of player details, financial transactions and game-play transactions.

3.3. Additional information

The MGA recognises that each setup is unique and may comprise different sets of complexities and different types of risks and risk levels. For this reason the MGA retains the right to request further information than that set by these guidelines and to require specific adaptations in order to comply with prevalent legislation at the time of review of the proposal, and the principles set out in this document.

Appendices

Appendix A | Risks

RISK #	RISK DESCRIPTION
1	Loss of governance. This risk also takes into consideration the changes to the CSP's terms and conditions and service levels whilst an operator is making use of its services. Such changes may also be a result of the CSP being acquired by a third party.
2	Inadequate maintenance of the systems and underlying infrastructure managed by the CSP.
3	Leakage of data during transfer within the cloud: between the operator and the cloud or between player and the cloud.
4	Insecure data storage.
5	Information not being erased thoroughly or in a timely manner by the CSP's systems following a command issued by the operator.
6	Unauthorised access to data through the management interface or any other system within the cloud or interfacing with the cloud.
7	Loss of privacy.
8	Unreliable service engine /APIs (Application Programming Interface) as well as isolation failure.
9	Loss incurred due to activities carried out by tenant(s) on the cloud.
10	Malicious activities by other tenant(s) of the cloud or employees of the CSP.
11	Failure by the CSP (or its providers) to provide an adequate level of service. This includes the risk of heightened dependency on the CSP as well as the complete cessation of a CSP service.
12	Increased dependency on internet connectivity for the operator to manage its operation.
13	Loss of intellectual property.
14	Lack of IT resource capacity.
15	Denial of service heightened due to use of the CSP services.

Appendix B | Terms and Definitions

Authority	Means the Malta Gaming Authority, also referred to as the 'MGA'.
Cloud Computing	The MGA considers that the definition adopted by the Cloud Security Alliance which states that 'cloud computing' is "… *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).* is the most suitable to apply and employ for the purposes of
Cloud Service Provider	Means any entity providing a Cloud Computing service, also referred to as CSP in these Guidelines.
Financial Data	Any data pertaining to the financial activity of a player.
Financial Database Server	Servers containing data pertaining to the financial activity of a player.
Gaming Database Server	Servers containing data which pertains to the gaming activity of a player.
Information Security Management System	As defined within ISO 27000.
Licensee	Means a person to whom the Authority has issued a remote gaming licence as per the Remote Gaming Regulations (S.L.438.04), and a licence or a remote gaming licence shall be construed accordingly.
Regulatory Data	Any form of data which the Authority may require to carry out its regulatory functions, including, but not limited to, player, game and financial data.
Remote Gaming Operator / Operator	An economic operator in Malta that is a licensee, or is in the process of obtaining a remote gaming licence.
Player Data	Any data which contributes or may contribute to the identification of a player.
Player Database Server	Servers containing data which contribute to or may contribute to the identification of a player.
Private Cloud	A cloud infrastructure that is for the exclusive use of a single tenant and where the service is completely isolated from third parties. It may be managed by the organisation or a third party, and may exist on-premises or off-premises.
Public Cloud	A cloud environment where the CSPs share their infrastructure and resources among various unrelated enterprises and individuals. Public Cloud Services are generally considered as more 'risky', although the security-related investment and the resources available to major Public Cloud Service Providers often exceed those of a typical licensee.

Technical Infrastructure	Refers to the entirety of the hardware and software resources across a network, used for the purpose of the licensed operation.
Virtual Private Cloud	A public cloud environment that simulates a private cloud through logical segregation.