GLI®

GAMING SECURITY FRAMEWORK

GLI-GSF-5

GAMING INFORMATION SECURITY (GIS) CONTROLS AUDIT – ONLINE GAMING CONTROLS

Version 1.0 – Published September 30, 2025

Contents

1. INTRODUCTION

1.1. General Statement

The integrity and accuracy of the operation of a Gaming Production Environment (GPE) is highly dependent upon operational procedures, configurations, and the network infrastructure. With ever emerging threats to gaming operations, Regulatory Bodies rely heavily on the expertise of a qualified Independent Security Firm (ISF) to perform gaming security assessments as an essential addition to the testing and certification of the Critical System Components of a GPE by an Independent Test Laboratory (ITL).

a. This module of the GLI Gaming Security Framework, GLI-GSF-5, establishes the additional Gaming Information Security (GIS) Controls to the GLI-GSF-1, which are necessary for auditing a Gaming Enterprise's Gaming Information Security Management System (GISMS) to ensure effective management of security in a Gaming Enterprise's GPE used in online gaming operations, using a gaming website, mobile application, or other digital platform, to offer interactive gaming, live studio gaming, internet lottery, online event wagering, or any other form of online gaming.
b. This module is intended to be evaluated as a companion to the GLI-GSF-1, which provides the common GIS Controls necessary for auditing a Gaming Enterprise's GISMS.
c. This module may be used alongside the GLI-GSF-2, which provides a benchmark for conducting Gaming Technical Security (GTS) assessments of a Gaming Enterprise's GPE.
d. Depending on the type of Gaming Enterprise, additional modules of the GLI-GSF may also apply.

NOTE: The entire GLI Gaming Security Framework (GLI-GSF) is available free of charge at www.gaminglabs.com.

1.2. Gaming Enterprise and Sensitive Data Management Role

Ensuring the security of a GPE is a collective responsibility that spans across the multiple entities which make up the Gaming Enterprise, such as the operator, and its suppliers, manufacturers, vendors, service providers, and other entities who have a role in overseeing or the operation of a GPE or providing services integral to its function. Each entity plays a crucial role in maintaining the confidentiality, integrity, availability, and accountability of the environment, especially when sensitive data is involved. For additional information, please refer to the "Gaming Enterprise and Sensitive Data Management Role" section of the GLI-GSF-1.

NOTE: This document is not intended to define which entities are responsible for meeting each GIS Control. It is the responsibility of the multiple entities which make up the Gaming Enterprise to agree on responsibility.

1.3. Gaming Production Environment (GPE)

A GPE refers to the operational setting where online gaming activities and related services are conducted, managed, and delivered to patrons in a live or real-time manner. It encompasses the physical and virtual infrastructure, gaming systems, software, and processes required to facilitate various forms of online gaming, such as interactive gaming (iGaming), interactive lottery (iLottery), online event wagering, and live studio gaming. The GPE also encompasses the backend systems, business applications, and infrastructure that interface and/or support online gaming activities. Key characteristics of a GPE are described in the "Gaming Production Environment (GPE)" section of the GLI-GSF-1.

1.4. Gaming Information Security Management System (GISMS)

A GISMS is a structured framework and set of processes designed to safeguard a Gaming Enterprise's sensitive data, assets, and Critical System Components within its GPE against unauthorized access, disclosure, alteration, or destruction. It encompasses policies, procedures, controls, and risk management practices specifically tailored to the unique challenges and regulatory requirements of the gaming industry by involving the identification of GIS risks, the implementation of appropriate controls and safeguards, ongoing monitoring and assessment of security measures, and continuous improvement to adapt to evolving threats and compliance requirements.

1.5. Framework Purpose

Ensuring the security and integrity of online gaming activities is paramount for upholding public confidence and trust in the sector. Therefore, Gaming Enterprises offering online gaming must establish and uphold a clearly defined and documented framework to attain and preserve public trust in their operations. The goal is to align GIS in such a way that gaming operations can function as other eCommerce operations to ensure a safe and stable environment with the secure features of operations in parallel industries.

1.6. Security Standards and Guidelines Consulted

Each module of the GLI-GSF is based on commonly used security standards and guidelines that provide an industry-accepted foundation developing effective GIS management practices. GLI acknowledges and thanks the Regulatory Bodies and other industry participants who have assembled rules, regulations, technical standards, and other documents which have been influential in the development of this document.

1.7. Adoption and Observance

This module of the GLI-GSF may be adopted in whole or in part by any Regulatory Body that wishes to implement a comprehensive set of GIS Controls to be applied for online gaming in conjunction with Common GIS Controls from the GLI-GSF-1.

2. ONLINE GIS (OGIS) CONTROLS AUDITS

2.1. Audit Overview

The OGIS Controls Audit is performed with the intent of identifying any actual or potential instances of non-compliance, vulnerabilities, or weaknesses, and assuring that the confidentiality, integrity, availability, and accountability of the information under the Gaming Enterprise's control are preserved. This methodology relies heavily on layered security to reduce the risk to computer and network systems by providing redundancy and reinforcing the overall security model, as several layers of security must be breached before a sensitive data store is accessed.

NOTE: The focus of the GIS guidance detailed in the GLI-GSF-5 is on specific information security controls for online gaming to apply in addition to the common information security controls for gaming in GLI-GSF-1, other evaluation methods are discussed in supporting modules of the GLI-GSF.

2.2. Audit Methods

The OGIS Controls Audit uses a range of assessment methods including the following methods, the results of which are used to support the determination of OGIS Control effectiveness over time:

a. Interview: A type of assessment method characterized by the process of conducting discussions with individuals or groups within a Gaming Enterprise to facilitate understanding, achieve clarification, or lead to the location of evidence.
b. Examine: A type of assessment method characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
c. Test: A type of assessment method characterized by the process of exercising one or more audit objects under specified conditions to compare actual with expected behavior.

2.3. Audit Tasks

The Appendix details the minimum OGIS Controls in more granular detail. Users of this document are directed to the Appendix of this module as well as the Appendix of the GLI-GSF-1 to ensure that no necessary GIS Controls are overlooked. The OGIS Controls listed in the Appendix are not exhaustive and in addition to the Common GIS Controls from the GLI-GSF-1, additional GIS Controls may be included based on regulatory requirements and scope of the assessment.

NOTE: Information on the high-level OGIS Controls Audit activities can be found within the “Audit Tasks” section in the GLI-GSF-1, including, but not limited to documentation review, interviews, controls assessment, GIS incident response plan assessment, and risk assessment.

2.4. Audit Frequency

OGIS Controls Audits must be performed by an ISF with the “Audit Frequency” expressed within the GLI-GSF-1. This may include additional audits as requested by the Regulatory Body or Gaming Enterprise, focused specifically on critical changes within the GPE that could affect the security of the GPE, that could allow access to sensitive data and/or Critical System Components, or any other changes impacting data flow or security posture.

NOTE: The Regulatory Body or Gaming Enterprise may also request a Vulnerability Scan or Gaming Technical Security (GTS) Testing be performed specifically on the critical changes and the Critical System Components affected by the changes. Please refer to GLI-GSF-2 for additional information.

2.5. Audit Reports

The results of an OGIS Controls Audit identify for Gaming Enterprises those areas in the operations where improvement should be considered and recommend strategies for improving those areas. The OGIS Controls Audit report must meet the requirements for “Audit Reports” as specified in the GLI-GSF-1.

2.6. Remediation

If the ISF's OGIS Controls Audit report recommends remediation, the Gaming Enterprise must provide the Regulatory Body and the ISF, if required by the Regulatory Body, with a remediation plan and any risk mitigation plans which detail the Gaming Enterprise's actions and schedule to implement the remediation steps.

NOTE: For additional information, please refer to the "Remediation" section of the GLI-GSF-1.

2.7. Independent Security Firm (ISF)

The OGIS Controls Audit must be carried out by individuals with sufficient qualifications, which means that the ISF must employ sufficiently qualified, competent, and experienced individuals. Unless otherwise specified by the Regulatory Body, these individuals must meet the qualifications specified for an "Independent Security Firm (ISF)". in the GLI-GSF-1.

APPENDIX: ONLINE GAMING INFORMATION SECURITY (OGIS) CONTROLS

In addition to the Common GIS Controls specified in the GLI-GSF-1 for GIG3 Gaming Enterprises, the following additional GIS Controls apply to Gaming Enterprises' GPEs offering online gaming.

OGIS-1	Signature Verification of Critical Control Programs
OGIS-1.1	**Signature Verification Procedure and Logging**
OGIS-1.1.1	Signatures of the Critical Control Programs shall be obtained from the GPE through a signature verification procedure, which must be executed under the following conditions: a. Upon installation or update to any Critical Control Programs; b. Upon system power-up or recovery from a shutdown state; c. At a minimum, once every 24 hours during normal operations; and d. Upon request (on demand).
OGIS-1.1.2	The signature verification procedure must include one or more analytical steps to compare the current signatures of the Critical Control Programs in the GPE against the signatures of the current approved versions.
OGIS-1.2	**Verification Audit Log**
OGIS-1.2.1	The output of the signature verification procedure must be recorded in a verification audit log, which comprises part of the sensitive data which must be recovered in the event of a disaster or equipment or software failure.
OGIS-1.2.2	The verification audit log must detail the following for each signature verification: a. The date and time of the verification; b. Identification of each verified Critical Control Program; c. The expected and generated signature results, including indication of any program error or signature mismatch; and d. When performed on demand, user account ID who initiated the verification procedure;
OGIS-1.2.3	The verification audit log must be accessible by the Regulatory Body in a format which permits analysis of each verification by the Regulatory Body.
OGIS-1.3	**Verification Failure**
OGIS-1.3.1	Any failure of signature verification of any Critical Control Program must require a notification of the verification failure to be communicated to the Gaming Enterprise.
OGIS-1.3.2	Where required by the Regulatory Body, the Gaming Enterprise must report the signature verification failure and corrective actions taken to the Regulatory Body without undue delay.
OGIS-2	**Back Office Administration**
OGIS-2.1	**Factor Authentication (MFA) Enforcement**
OGIS-2.1.1	Back Office Administration Applications must support enforcement of MFA for all privileged accounts used by individuals for accessing the applications where possible. This includes administrative, operational, system, and support accounts with elevated permissions.
OGIS-2.1.2	When MFA is enforced, the MFA must use at least two distinct authentication factors (e.g., password and hardware token) to reduce the risk of unauthorized access due to compromised credentials.
OGIS-2.1.3	Where implementation of MFA is not possible (e.g. service accounts), privileged accounts must have compensating controls such as strong authentication, privileged account management, conditional access controls, and extra monitoring.
OGIS-2.2	**Vendor Support Access Monitoring**
OGIS-2.2.1	All vendor access to Back Office Administration Applications, whether remote or on-site, for maintenance, troubleshooting, or support purposes must be strictly controlled, monitored, and logged by the Gaming Enterprise.
OGIS-2.2.2	Vendor access must only be granted on a temporary, as-needed basis through secure communication channels.
OGIS-2.2.3	All vendor activities performed during such access must be fully logged and auditable to ensure accountability and support monitoring, analysis, and forensic review.
OGIS-2.2.4	All changes to vendor access, including additions, modifications, or removals, must be formally documented and recorded to maintain an auditable trail of access management activities.
OGIS-2.2.5	The GPE must include a mechanism to immediately revoke vendor access in the event of a GIS incident, ensuring prompt mitigation of potential security or operational risks.

OGIS-2.3	**Role-Based Access Controls (RBAC) and Least Privilege**
OGIS-2.3.1	Back Office Administration Applications must implement RBAC to assign permissions based on users' job responsibilities. Changes to RBAC must be documented and recorded.
OGIS-2.3.2	Access must follow the principle of least privilege, ensuring users have only the minimum permissions necessary to perform their duties.
OGIS-2.3.3	Back Office Administration Applications must enforce a segregation of duties to prevent the same individual from performing conflicting tasks (e.g., initiating and approving transactions).
OGIS-2.4	**Network Access Restrictions**
OGIS-2.4.1	Access to Back Office Administration Applications must be restricted to trusted and authorized networks, implementing at least one of the following controls to enforce this restriction: IP whitelisting, firewalls, network segmentation, or secure Virtual Private Network (VPN) access. a. Public networks and untrusted devices must be explicitly denied access. b. All other not explicitly authorized traffic must be implicitly denied access. c. Zero trust solutions must continuously verify the trustworthiness of users and devices prior to granting access, ensuring that no implicit trust is granted based on network location or other assumed factors. d. Where implementation of the above controls is not feasible due to product configuration, additional compensating controls must be applied and documented.
OGIS-2.4.2	Network access controls must be regularly reviewed and updated to ensure continued alignment with the security posture of the Gaming Enterprise.
OGIS-2.5	**Session and Account Management**
OGIS-2.5.1	Back Office Administration Applications must be configured to prohibit simultaneous logins from the same user account across multiple devices or sessions.
OGIS-2.5.2	Where technically feasible, existing active sessions must be terminated when a duplicate login is attempted in order to prevent simultaneous unauthorized access and protect account integrity.
OGIS-3	**Server-Side Integrity and Programming Security**
OGIS-3.1	**Server-Side Validation of Gaming Logic**
OGIS-3.1.1	All critical gaming logic and state transitions (e.g., scoring, balance updates, win/loss resolution) must be validated on the server-side, regardless of client input.
OGIS-3.1.2	Inputs received from the gaming website, mobile application, or other digital platform must be checked for integrity, authentication, and logical consistency before any state change is applied.
OGIS-3.2	**Execution Control and External Code Restrictions**
OGIS-3.2.1	The Gaming Enterprise must implement and maintain robust mechanisms designed to prevent the execution of potentially harmful or unauthorized code introduced through mobile devices, removable media, or other external sources.
OGIS-3.2.2	The Gaming Enterprise must restrict critical servers to running only approved and verified applications, blocking all unapproved or unauthorized code from execution (e.g., implementation of application whitelisting that only allows pre-approved or “whitelisted” software applications to run on a system).
OGIS-3.2.3	The Gaming Enterprise must enforce policies that disable or limit the ability to run code from external or untrusted devices, including disabling autorun features and restricting script execution.
OGIS-3.3	**Policy Enforcement**
OGIS-3.3.1	The Gaming Enterprise must establish and enforce policies governing the use of mobile devices and external media in servers running Critical Control Programs (e.g., only managed mobile devices can connect to the network, and USB drives are blocked on critical servers). This may include Mobile Device Management (MDM), network access controls, or server-level restrictions to prevent unauthorized connections or data transfers.
OGIS-3.3.2	The Gaming Enterprise must restrict or prohibit the connection or use of unauthorized mobile devices and external media to prevent introduction of untrusted or harmful code.
OGIS-3.3.3	The Gaming Enterprise must define procedures and secure methods for introducing any external code, software, or updates to ensure integrity and compliance with security standards.
OGIS-3.3.4	The Gaming Enterprise must establish requirements for device authentication, scanning, and validation before any external media or code is allowed on Critical System Components.
OGIS-3.4	**GPE Monitoring and GIS Incident Response**
OGIS-3.4.1	Continuous monitoring mechanisms must be implemented to detect, alert on, and record any attempts at unauthorized code execution, supporting timely response, analysis, and forensic investigation of potential GIS incidents.

OGIS-3.4.2	The Gaming Enterprise must have procedures in place to promptly address any GIS Incidents related to mobile code or external executable threats.
OGIS-3.5	**Cloud and Virtualized Environment Security**
OGIS-3.5.1	Each server instance deployed within a cloud or virtualized environment must be dedicated to a single critical function (e.g., the database server may not host the web or application services). This approach ensures logical separation of duties, limits the blast radius of potential security incidents, and aligns with the principle of least privilege.
OGIS-3.5.2	The Gaming Enterprise must implement technical and administrative controls to enforce role separation between server instances by isolating functions. This includes using distinct virtual machines, containers, or services for each function (e.g., database, application, web server), and applying workload-specific configurations, access controls, and monitoring to each instance.
OGIS-4	**Application Protection Mechanisms**
OGIS-4.1	**Secure Communications in Mobile Applications**
OGIS-4.1.1	Mobile applications must ensure secure communication between the client and the server. This can be achieved through SSL/TLS certificate pinning or equivalent measures, such as certificate transparency monitoring or dynamic pinning frameworks, which provide comparable protection against “Man-In-The-Middle” attacks while supporting safe certificate or encryption key management.
OGIS-4.1.2	Mobile applications must be designed to terminate network connections immediately if the pinned certificate or encryption key does not match the expected value.
OGIS-4.1.3	All certificate or encryption key validation failures must be logged to support monitoring, analysis, and forensic investigation purposes, ensuring traceability of GIS incidents and potential system compromises.
OGIS-4.2	**Jailbreak/Root Detection on Mobile Devices**
OGIS-4.2.1	As part of a layered defense strategy, mobile applications may implement jailbreak detection (iOS) and root detection (Android) to prevent execution on compromised devices. Detection should cover common techniques, tools, and system anomalies indicative of tampering.
OGIS-4.2.2	If a mobile device is determined to be rooted or jailbroken, the application must restrict access to sensitive features or terminate operation.
OGIS-4.3	**Code Obfuscation for Mobile Applications**
OGIS-4.3.1	The mobile application codebase must implement code obfuscation to protect against reverse engineering. This includes, but is not limited to: a. Renaming classes, variables, and methods to non-descriptive identifiers; b. Modifying control flows to make the program logic harder to follow; and c. Applying string encryption or hiding critical resources.
OGIS-4.3.2	The code obfuscation processes must be integrated into the automated build pipeline to ensure that every production build is properly obfuscated before release.
OGIS-4.3.3	Tamper-detection mechanisms must be implemented to alert authorized personnel if the mobile application is altered post-distribution, ensuring integrity throughout the software lifecycle.
OGIS-4.4	**Detection and Prevention of Password Stuffing Attacks**
OGIS-4.4.1	The Gaming Enterprise must implement mechanisms to detect patterns consistent with password stuffing, such as high-volume login attempts using varied credentials from a single IP address or device.
OGIS-4.4.2	Preventive measures must be enforced on authentication endpoints (e.g., CAPTCHA challenges, rate limiting, account lockout policies, credential stuffing detection logic, etc.).
OGIS-4.5	**Bot Mitigation Solutions**
OGIS-4.5.1	The GPE must integrate a bot mitigation solution to detect and block automated traffic attempting to perform abusive, fraudulent, or otherwise unauthorized actions.
OGIS-4.5.2	Bot mitigation solutions must include behavioral analysis, device fingerprinting, and challenge-response mechanisms to differentiate between human users and automated scripts.
OGIS-4.6	**API Security**
OGIS-4.6.1	All APIs supporting the gaming website, mobile application, or other digital platform must adhere to the OWASP API Security Top 10 Best Practices, including authentication, rate limiting, data validation, and error handling.
OGIS-4.6.2	The Gaming Enterprise must regularly perform API security testing, including in the development phase, (e.g., penetration tests, static/dynamic analysis) and deploy API gateways or web application firewalls (WAFs) to enforce API security policies and monitor real-time traffic.

OGIS-4.7	**Security Architecture**
OGIS-4.7.1	The network segments that comprise the infrastructure of the gaming website, mobile application, or other digital platform must be isolated from each other.
OGIS-4.7.2	Communication between segments shall be explicitly restricted to only the protocols, hosts, and services required for operational functionality.
OGIS-4.7.3	For a zero-trust network, all inter-segment traffic must be authenticated, authorized, and continuously monitored to prevent unauthorized access and lateral movement within the network.
OGIS-4.7.4	The gaming website, mobile application, or other digital platform must be protected by a WAF or an equivalent control that provides comparable protection against web-based attacks, including but not limited to injection attacks, cross-site scripting, and other common application-layer threats.
OGIS-4.7.5	The WAF or equivalent control must be regularly monitored for events of interest and updated to ensure the latest attack vectors are configured to be monitored.
OGIS-5	**Distributed Denial of Service (DDoS) Protection Controls**
OGIS-5.1	**Multi-Layer Rate Limiting and Throttling**
OGIS-5.1.1	Rate limiting must be enforced at multiple tiers must be enforced of the GPE architecture to identify and throttle abusive request patterns and mitigate service degradation: a. Network level: Firewalls and ingress controllers must enforce thresholds on connections or packets per source (e.g., per IP address). b. API gateway level: API gateways must, where possible, limit the number of calls per client, incorporating burst handling and back-off mechanisms. c. Application level: Application logic must detect and suppress excessive or abusive use of specific endpoints to prevent resource exhaustion.
OGIS-5.1.2	Rate limiting must be adaptive to changing traffic patterns and system load, and all violations of defined thresholds must be logged for monitoring, analysis, and forensic purposes.
OGIS-5.2	**IP Obfuscation and DDoS Mitigation**
OGIS-5.2.1	The public IP addresses of gaming servers, APIs, administrative panels, and other Critical System Components must be obfuscated to prevent direct targeting of infrastructure. This obfuscation may be achieved through, but is not limited to: a. Reverse proxies, Content Delivery Networks (CDNs), or cloud-based load balancers (e.g., placing a CDN in front of a gaming server to handle requests while hiding the origin server IP address; and b. Network Address Translation (NAT) and overlay networks (e.g., using private IP addressing combined with NAT, or implementing software-defined overlay networks, to mask the true origin location and addressing of backend servers.
OGIS-5.2.2	Third-party DDoS protection services must be integrated into the GPE to enhance resilience and maintain availability. Integration must provide the following capabilities: a. Detect and absorb volumetric, protocol, and application-layer attacks (e.g., automatically identifying and blocking excessive Hypertext Transport Protocol (HTTP) requests targeting an API); b. Ensure malicious traffic is filtered upstream before reaching the GPE (e.g., using scrubbing centers to clean traffic); c. Maintain business continuity through automatic failover and global edge networks (e.g., redirecting traffic to alternative edge nodes if a regional node is under attack); and d. Validate service-level agreements (SLAs) and GIS response procedures with Service Providers (e.g., periodically testing failover and response times as per contractual SLAs.

DEFINITIONS OF TERMS

Term	Descriptions
Access	Ability to make use of any GPE resource.
Access Control	The process of granting or denying specific requests for obtaining and using sensitive data and related services specific to a system; and to enter specific physical facilities which houses critical network or system infrastructure.
Administrative Controls	Policies, procedures, and guidelines implemented by a Gaming Enterprise to manage its GISMS.
Application	Computer software that is designed to help a user perform a specific task.
Audit Log	An auditable record of actions, events, or changes within a GPE, capturing details such as user activities, access attempts, alterations, and system operations to ensure security, compliance, and accountability during a given period.
Authentication	Verifying the identity of a user, process, software package, or device, often as a prerequisite to allowing access to resources in the GPE.
Authentication Credentials	Any passwords, multi-factor authentication, digital certificates, PINs, biometrics, security questions and answers, and any other account access methods (e.g., magnetic swipe, proximity cards, embedded chip cards).
Availability	Ensuring timely and reliable access to and use of information.
Back Office Administration Application	A secure, centralized software system used by Gaming Enterprises and Regulatory Bodies to manage, monitor, and support the operational, financial, compliance, and customer service functions of a GPE, such as identification verification, anti-money laundering, and regulatory reporting systems.
Biometrics	A biological identification input, such as fingerprints, retina patterns, facial recognition data, or voiceprints.
Business Applications	Applications operating as a shared service for users to collect, process, maintain, use, share, disseminate, or dispose of sensitive data within the GPE for compliance auditing and GIS incident response purposes.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical Control Program	Software programs that control behaviors relative to any applicable technical standard and/or regulatory requirement, such as executables, libraries, gaming or system configurations, operating system files, components that control required system reporting, and database elements that affect gaming or system operations.
Critical System Component	Any hardware, software, Critical Control Programs, communications technology, other equipment or components implemented in a GPE to allow patron participation in gaming, and whose failure or compromise can lead to loss of patron entitlements, government revenue or unauthorized access to data used for generating reports for the Regulatory Body. Examples of Critical System Components include, but are not limited to: • Components which record, store, process, share, transmit, or retrieve sensitive data. • Components that could impact the security of sensitive data or the GPE. • Components which generate, transmit, or process random numbers used to determine the outcome of games and events. • Components which store results or the current state of a patron's game, wager, or available funds. • Points of entry to and exit from the above components, including other systems which communicate directly with Critical System Components. • Communications technology and networks which transmit sensitive data, including network communication equipment (NCE) and network security controls. • Components that provide security services, including authentication servers, access control servers, security information and event management (SIEM) systems, physical security systems, surveillance

Term	Descriptions
	systems, multi-factor authentication (MFA) systems, anti-malware/anti-virus systems. • Components that facilitate segmentation, including internal network security controls. • Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. • Cloud infrastructure and components, both external and on premises, and including instantiations of containers or images, virtual private clouds, cloud-based identity and access management, components residing on premises or in the cloud, service meshes with containerized applications, and container orchestration tools. • Server types including web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name Service (DNS). • End-user devices, such as computers, laptops, workstations, administrative workstations, tablets, and mobile devices. • Applications, software, and software components, serverless applications, including all purchased, subscribed (e.g., Software-as-a-Service), custom, and in-house built applications, including internal and external (e.g., Internet) applications. • Tools, code repositories, and systems that implement software configuration management or for deployment of objects to the GPE or to components that can impact the GPE. • Corporate networks and systems that interface with the GPE and from which attackers could use to move laterally into the GPE (e.g., corporate casinos' networks and online operators' corporate networks). • Any other component deemed critical to the GPE by the Regulatory Body or the Gaming Enterprise.
Distributed Denial of Service (DDoS)	A type of attack where multiple compromised systems, usually infected with a destructive software program, are used to target a single system. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.
Domain	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
Domain Name Service (DNS)	The globally distributed internet database which (amongst other things) maps machine names to IP numbers and vice-versa.
Encryption	The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people. Where encryption is not possible due to a technology or performance limitation, other reasonable protective measures must be implemented in its place and reviewed on a case-by-case basis.
Encryption Key	A key that has been encrypted in order to disguise the value of the underlying plaintext.
Firewall	A component of a computer system or network that is designed to block unauthorized access or traffic while still permitting outward communication.
Gaming Enterprise	An operator, and any suppliers, manufacturers, vendors, service providers, and/or other entities who have a role in overseeing the operation of a GPE, or providing services integral to its function, including the management of sensitive data.
Gaming Information Security (GIS)	Protecting sensitive data and Critical System Components from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, availability, and accountability.
Gaming Information Security Management System (GISMS)	A defined, documented management system that consists of a set of policies, processes, and systems to manage risks to a Gaming Enterprise's sensitive data, assets, and Critical System Components within a GPE, with the objective of ensuring acceptable levels of GIS risk.

Term	Descriptions
Gaming Production Environment (GPE)	The operational setting where gaming activities and related services are conducted, managed, and delivered to patrons in a live or real-time manner. It encompasses the physical and virtual infrastructure, gaming systems, software, and processes required to facilitate various forms of gaming and/or manage sensitive data, as well as the backend systems and infrastructure that interface and/or support gaming activities.
Gaming Systems	Critical System Components that are relative to any applicable technical standard and/or regulatory requirement for gaming activities.
Gateway	Any device, system, or software application that can perform the function of translating data from one format to another. The key feature of a gateway is that it converts the format of the data, not the data itself.
GIS Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, availability, or accountability of a GPE or the sensitive data the GPE processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Examples of reportable GIS incidents include, but are not limited to: • Unauthorized access to sensitive data or Critical System Components. • Malicious code execution or ransomware infection within the GPE. • Loss, theft, or unauthorized disclosure of PII. • System outages or disruptions affecting the integrity or availability of gaming operations for a defined period (e.g., more than 15 minutes). • Detection of tampering, manipulation, or attempted compromise of gaming software or hardware. • Repeated or systemic failed login attempts indicative of a brute-force attack. • Compromise or misuse of administrative credentials or security certificates. • Security configuration changes that were made outside of authorized change management processes.
GIS Incident Response Plan	The documentation of a predetermined set of instructions or procedures when a malicious cyberattack is encountered against a Gaming Enterprise's GPE.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Internet Protocol Address (IP Address)	A unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.
Key	A value used to control cryptographic functions, such as encryption, decryption, signatures, hashing, etc.
Key Management	Activities involving the handling of encryption keys and other related security parameters (e.g., passwords) during the entire lifecycle of the keys, including their generation, storage, establishment, entry, and output, and zeroization.
Layered Security	A defense approach that uses multiple independent protections across a system, like firewalls, authentication, encryption, and monitoring, so that an attacker must bypass several layers before accessing sensitive data or Critical System Components.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, availability, or accountability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
"Man-In-The-Middle" Attack	An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Also known as an "On-Path" attack.
Message Authentication	A security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.

Term	Descriptions
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Mobile Code	Executable code that moves from computer to computer, including both legitimate code and malicious code such as computer viruses.
Microservice	A small, independent piece of software that performs a specific function within a larger system. Each microservice runs on its own, communicates with others through secure connections, and can be updated or replaced without disrupting the whole system.
Multi-Factor Authentication (MFA)	A type of authentication which uses two or more of the following to verify a user's identity: • Information known only to the user (e.g., a password, PIN, or answers to security questions); • An item possessed by a user (e.g., an electronic token, physical token, or an identification card); and • A user's biometric data (e.g., fingerprints, retina patterns, facial recognition data, or voiceprints).
Network Communication Equipment (NCE)	Communications technology that controls data communication in a system including, but not limited to, NICs, cables, switches, bridges, hubs, routers, WAPs, and telephones, VoIP network devices, network appliances, and other security appliances.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Personally identifiable information (PII)	Sensitive data that could potentially be used to identify a particular person. Examples include a legal name, date of birth, place of birth, government identification number (social security number, taxpayer identification number, passport number, or equivalent), personal financial information (credit or debit instrument numbers, bank account numbers, etc.), or other personal information if defined by the Regulatory Body.
Personal Identification Number (PIN)	A numerical code associated with an individual which allows secure access to a domain, account, network, system, etc.
Protocol	A set of rules and conventions that specify information exchange between devices, through a network or other media.
Regulatory Body	The governmental body or equivalent which regulates or controls the operations of gaming.
Risk	The likelihood of a threat being successful in its attack against a network or system within the GPE.
Risk Assessment	Identifying, analyzing, and prioritizing threats and vulnerabilities to a Gaming Enterprise's operations or assets, or to individuals or other entities, resulting from impairment of the confidentiality, integrity, availability, and accountability of sensitive data or the reliability, security, or capacity of the GPE.
Sensitive Data	Information that needs to be handled in a secure manner, including but not limited to, as applicable: • Audit logs and system databases recording information used to determine outcome, payment, redemption, and the tracking of patron information; • Accounting and significant event information related to the Critical System Components of the GPE; • RNG seeds and any other information which affects outcomes of games and wagers; • Encryption keys, where the implementation chosen requires transmission of keys; • Validation numbers associated with patron accounts, wagering instruments, and any other gaming transactions; • Transfers of funds to and from patron accounts, electronic payment accounts, and for the purposes of gaming; • Software packages within the GPE;

Term	Descriptions

	• Any location data related to employee or patron activity (e.g. account management, online gaming, etc.);
	• Any of the following information recorded for any employee or patron:
	  • Government identification number (social security number, taxpayer identification number, passport number, or equivalent);
	  • Personal financial information (credit or debit instrument numbers, bank account numbers, etc.);
	  • Authentication credentials in relation to any user account or patron account;
	  • Any other personally identifiable information (PII) which needs to be kept confidential; and
	• Any other data deemed sensitive by the Regulatory Body or the Gaming Enterprise.

Server	A running instance of software that is capable of accepting requests from clients, and the computer that executes such software. Servers operate within a Client-Server Architecture, in which "servers" are computer programs running to serve the requests of other programs ("clients").
Service Providers	Entities that offer platforms, software, and services to Gaming Enterprises. Examples include IT consultants, managed service provider, Software as a Service (SaaS) platforms, and cloud service providers. Third-party providers and vendors are also considered Service Providers.
Signature Verification	Ensuring by electronic signature checking that any software package is an authentic copy of the software created by its manufacturer and, if applicable, an exact copy of the software as certified by the Independent Test Laboratory (ITL).
Technical Controls	The security mechanisms implemented within Gaming Production Environment's systems and infrastructure to protect against unauthorized access, data breaches, and other security threats.
Threat	Any circumstance or event with the potential to adversely impact network operations (including mission, functions, image, or reputation), assets, or individuals through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service; the potential for a threat-source to successfully exploit a particular vulnerability; any potential danger to a network that someone or something may be able to identify as being vulnerable, and therefore seek to exploit.
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
Virtual Private Network (VPN)	A logical network that is established over an existing physical network and which typically does not include every node present on the physical network.
Virus	A self-replicating program, typically with malicious intent, that runs and spreads by modifying other programs or files.
Vulnerability	Software, hardware, or other weaknesses in a network or system that can provide a "door" to introducing a threat.