GLI®

GAMING SECURITY FRAMEWORK

GLI-GSF-5

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

Version 1.0 DRAFT – Published August 22, 2025

GAMING LABORATORIES INTERNATIONAL®

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 online games, live studio gaming, internet lottery, online event wagering, or any other form of interactive 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 integrity, availability, and confidentiality 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, systems, software, and processes required to facilitate various forms of online gaming, such as interactive gaming, interactive lottery, 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 was 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 CONTROLS AUDITS

2.1. Audit Overview

The Online GIS Controls Audit is performed with the intent of identifying any actual or potential instances of non-compliance, vulnerabilities, or weaknesses, and assuring that the integrity, confidentiality, and availability 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

An Online GIS Controls Audit uses a range of assessment methods including the following methods, the results of which are used to support the determination of Online GIS Control effectiveness over time. Additional information regarding the "Audit Methods" can be found in the GLI-GSF-1.

2.3. Audit Tasks

The Appendix details the minimum Online GIS Controls in more granular detail. Users of this document are directed to the Appendix as well as the Appendix of the GLI-GSF-1 to ensure that no necessary GIS Controls are overlooked. The Online GIS 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. Information on the high-level Online GIS Controls Audit activities can be found within the "Audit Tasks" section in the GLI-GSF-1.

2.4. Audit Frequency

In addition, to the timing of Online GIS Controls Audits expressed in the "Audit Frequency" section of the GLI-GSF-1, the Gaming Enterprise must, as a rule, have additional Online GIS Controls Audits performed by an ISF after any critical changes that could affect the security of the GPE or allow access to sensitive data and/or Critical System Components. These audits may be focused specifically on the critical changes and the Critical System Components affected by the changes. These critical changes may include, but are not limited to

a. Deployment of New Platforms
   i. Integration of new or heavily modified Remote Gaming Servers or Aggregators, Jackpot Controllers, Patron Account Management Systems, Event Wagering Engines, and other Online Gaming Systems
   ii. Launch of new gaming verticals (e.g., event wagering, live studio gaming)
   iii. Platform expansion to gaming websites, mobile applications, smart TVs, or consoles
b. Backend Infrastructure and Architecture Changes
   i. Migration to a new cloud or hosting provider
   ii. Adoption of containerization, microservices, or serverless models
   iii. Deployment of new data centers (especially cross-jurisdictional)
c. Modifications to Sensitive Data Storage and Handling
   i. Changes to sensitive data storage, logging, encryption, or retention
   ii. Shifts in sensitive data residency (e.g., moving primary sensitive data storage from one location to another)
d. Major Codebase or Platform Updates
   i. Significant updates to the core Critical System Components
   ii. Use of new development frameworks or programming languages
   iii. Integration of AI-based features (e.g., behavior analysis, fraud detection)
e. Changes to Payment Systems or Financial Transactions
   i. Integration of new payment processors, wallets, or banking APIs
   ii. Introduction of alternative payment methods
   iii. Changes to withdrawal, deposit, or payout mechanisms
   iv. Adjustment to system-wide financial transaction logic

f. Changes to Patron Identification and Location Detection
    i. Introduction of new identity verification processes (KYC) and location detection methods
    ii. Changes to authentication credential policies, multi-factor authentication (MFA), and location data sources (e.g. Wi-Fi, GSM, GPS)
    iii. Integration with third-party identity verification providers and third-party location detection providers

g. Incident Response Triggers
    i. Any data breach, service compromise, or fraud event
    ii. Detection of malware, cheating software, or collusion activity

h. Any other changes deemed critical by the Regulatory Body

NOTE: Certain critical changes may also require 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 Online GIS Controls Audit identify for Gaming Enterprises those areas in the operations where improvement should be considered and recommend strategies for improving those areas. The Online GIS Controls Audit report must meet the requirements of "Audit Reports" are specified in the GLI-GSF-1.

2.6. Remediation

If the ISF's Online GIS 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. For additional information, please refer to the "Remediation" section of the GLI-GSF-1.

2.7. Independent Security Firm (ISF)

The Online GIS 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: a. Operate independently of any process or security software within the GPE; and b. Include one or more analytical steps to compare the current signatures of the Critical Control Programs in the GPE with the signatures of the current approved versions of the Critical Control Programs.
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; 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	MFA must be enforced for all privileged accounts accessing Back Office Administration Application. This includes administrative, operational, and support accounts with elevated permissions.
OGIS-2.1.2	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-2.2	**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	Access must only be granted on a temporary, as-needed basis through secure channels, and activity must be fully auditable.
OGIS-2.3	**Role-Based Access Control and Least Privilege**
OGIS-2.3.1	Back Office Administration Applications must implement Role-Based Access Controls (RBAC) to assign permissions based on users' job responsibilities.
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	Segregation of duties must be enforced 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 using IP whitelisting, firewalls, and network segmentation.
OGIS-2.4.2	Public networks and untrusted devices must be explicitly denied access.
OGIS-2.4.3	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 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, active sessions must be terminated if a duplicate login is attempted.
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 execution to approved and verified applications only, blocking all other code from running on critical servers.
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 where Critical Control Programs operate.
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	**Monitoring and Incident Response**
OGIS-3.4.1	Continuous monitoring must be implemented to detect any unauthorized code execution attempts.
OGIS-3.4.2	The Gaming Enterprise must have procedures in place to promptly address any security events 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. 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. 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.
OGIS-4	**Application Protection Mechanisms**
OGIS-4.1	**SSL Pinning in Mobile Applications**
OGIS-4.1.1	Mobile applications must implement SSL pinning to ensure secure communication between the client and the server.
OGIS-4.1.2	Mobile applications must be designed to terminate network connections immediately if the pinned certificate or key does not match.
OGIS-4.1.3	Certificate validation failures must be logged for monitoring and forensic purposes.

OGIS-4.2	**Jailbreak/Root Detection on Mobile Devices**
OGIS-4.2.1	Mobile applications must 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 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 use code obfuscation techniques to make reverse engineering of the binary difficult by altering class, variable, and method names, and restructuring control flows.
OGIS-4.3.2	The obfuscation process must be included in the automated build pipeline to ensure every production build is properly obfuscated before release, and tamper-detection mechanisms should alert if the mobile application has been altered post-distribution.
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, including CAPTCHA challenges, rate limiting, account lockout policies, and credential stuffing detection logic, must be enforced on authentication endpoints.
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 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 app, or 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 and only allow needed communication on specific protocols and hosts.
OGIS-4.7.2	The gaming website, mobile application, or other digital platform must be protected by a WAF or equivalent.
OGIS-4.7.3	The WAF or equivalent 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 at multiple tiers must be enforced to throttle abusive request patterns and mitigate service degradation: a. Network level: Firewalls and ingress controllers should cap connections or packets per IP. b. API gateway level: Limit API calls per client, with burst handling and back-off mechanisms. c. Application level: Apply logic to detect and suppress excessive use or abuse of specific endpoints.
OGIS-5.1.2	Rate limiting must be adaptive and log violations for analysis.
OGIS-5.2	**IP Obfuscation and DDoS Mitigation**
OGIS-5.2.1	The public IP addresses of gaming servers, APIs, admin panels, and other Critical System Components must be obfuscated using: a. Reverse proxies, Content Delivery Networks (CDNs), or cloud load balancers; and b. Network Address Translation (NAT) and overlay networks to mask true origin infrastructure.
OGIS-5.2.2	Third-party DDoS protection services must be integrated to: a. Detect and absorb volumetric, protocol, and application-layer attacks; b. Ensure traffic scrubbing is performed upstream before reaching the GPE; c. Maintain business continuity through automatic failover and global edge networks; and d. Validate service-level agreements (SLAs) and incident response procedures with Service Providers.

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.
Biometrics	A biological identification input, such as fingerprints, retina patterns, facial recognition data, or voiceprints
Bridge	Divides networks to reduce overall network traffic. A bridge allows or prevents data from passing through it by reading the MAC address.
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 security incident response purposes
Business Continuity and Disaster Recovery Plan	A plan for processing critical applications and preventing loss of data in the event of a major hardware or software failure or destruction of facilities.
Cache Poisoning	An attack where the attacker inserts corrupt data into the cache database of the Domain Name Service (DNS).
Communications Technology	Any method used, and the components employed, to facilitate the transmission and receipt of information, including transmission and reception by systems using wire, wireless, cable, radio, microwave, light, fiber optics, satellite, or computer data networks, including the Internet and intranets.
Compliant	The policy and evidence viewed was considered to be fully compliant with the GLI-GSF.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Contingency Plan	Management policy and procedures designed to maintain or restore gaming operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
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:

Term	Descriptions
	• 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 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 System (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
Cryptographic Module	Hardware, software, firmware, or combination thereof that implement cryptographic functions such as encryption, decryption, signatures, hashing, and key management. The primary purpose of a cryptographic module is to provide secure processing and storage of keys and operations.
Data Integrity	The property that data is both accurate and consistent and has not been altered in an unauthorized manner in storage, during processing, and while in transit.
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.

Term	Descriptions
Domain Name Service (DNS)	The globally distributed internet database which (amongst other things) maps machine names to IP numbers and vice-versa.
Dynamic Host Configuration Protocol (DHCP)	A network service that allows devices to request a configuration from a central point. First a request is broadcasted over the network segment, then any servers respond to that specific machine with an address, how long that address is good for, and other pertinent details.
Effective Bandwidth	The amount of data that actually can be transferred across a network per unit of time. The effective bandwidth through the Internet is usually considerably lower than the bandwidth of any of the constituent links.
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.
Externally-Exposed Applications	Applications that are public facing and discoverable through reconnaissance and network scanning from the public internet outside of the enterprise's network. This does not apply to applications intended for patron use.
Externally-Exposed Enterprise Assets	Assets that are public facing and discoverable through Domain Name System reconnaissance and network scanning from the public internet outside of the enterprise's network. This does not apply to assets intended for patron use.
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 integrity, confidentiality, and availability.
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.
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, 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 System	Critical System Component 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 Policy	A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.
GIS Incident	An occurrence that actually or potentially jeopardizes the integrity, confidentiality, or availability of an 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.
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

Term	Descriptions
Group Membership	A method of organizing user accounts into a single unit (by job position) whereby access to system functions may be modified at the unit level and the changes take effect for all user accounts assigned to the unit.
Hypertext Transport Protocol (HTTP)	The underlying protocol used to define how messages are formatted and transmitted, and what actions servers and browsers must take in response to various commands.
Hub	Connects devices on a twisted-pair network. A hub does not perform any tasks besides signal regeneration.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Internet	An interconnected system of networks that connects computers around the world via TCP/IP.
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.
Intrusion Detection System/Intrusion Prevention System (IDS/IPS)	A system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Used in computer security, intrusion detection refers to the process of monitoring computer and network activities and analyzing those events to look for signs of intrusion in the GPE.
IP Security (IPSec)	A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of encryption keys to be used during the session.
Kerberos	A network authentication protocol designed to provide strong authentication for client/server applications by using secret-key encryption.
Key	A value used to control cryptographic functions, such as decryption, 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.
Link Utilization	The percentage time that a communications link is engaged in transmitting data.
Major Non-Conformity	A fundamental failing (systematic) has been identified that affects several GIS Controls and means that the overall security policies cannot be adhered to. It may be either: • A number of minor non-conformities against one control can represent a total failure of the system and thus be considered a major non-conformity; • Any non-conformity that would result in the probable shipment of a non-conforming product. A condition that may result in the failure or materially reduce the usability of the products or services for their intended purpose; or • A non-conformity that judgment and experience indicate is likely either to result in the failure of the system or to materially reduce its ability to assure controlled processes and products.
Malfunction	When a Critical System Component does not operate as intended.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the integrity, confidentiality, or availability 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.

Term	Descriptions
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.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Minor Non-Conformity	A GIS Control has not been addressed or is not compliant with the GLI-GSF (non-systematic) and that judgment and experience indicate is not likely to result in the failure of the system or reduce its ability to assure controlled processes or products. It may be either: • A failure in some part of the system relative to a control; or • A single observed lapse in following one item of the system.
Mobile Code	Executable code that moves from computer to computer, including both legitimate code and malicious code such as computer viruses.
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, wireless access points, and telephones, VoIP network devices, wireless access points, network appliances, and other security appliances.
Network Interface Card (NIC)	The mechanism by which terminals and systems connect to the network. NICs can be add-in expansion cards, PCMCIA cards, or built-in interfaces.
Observation	A finding worth noting for possible improvement to meet industry best practices.
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 and which allows secure access to a domain, account, network, system, etc.
Physical and Environmental Controls	The measures implemented to protect physical assets, facilities, and environmental conditions that house the Gaming Production Environment's systems and infrastructure.
Port	A physical entry or exit point of a module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).
Proxy	An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the internal network.
Protocol	A set of rules and conventions that specifies 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.
Remote Access	Any access from outside the system or system network including any access from other networks within the same site or venue.

Term	Descriptions
Risk	The likelihood of a threat being successful in its attack against a network or system.
Router	Connects networks together. A router uses the software-configured network address to make forwarding decisions.
Secure Communication Protocol	A communication protocol that provides the appropriate confidentiality, authentication, and content integrity protection.
Secure Shell (SSH)	Allows tunneling any other protocol in a secure manner.
Security Certificate	Information, often stored as a text file that is used by the Transport Socket Layer (TSL) Protocol to establish a secure connection. In order for a TSL connection to be created, both sides must have a valid Security Certificate.
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; • 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.
Service Set Identifier (SSID)	A name that identifies a particular 802.11 wireless LAN.
Shellcode	A small piece of code used as a payload in the exploitation of security. Shellcode exploits vulnerability and allows an attacker the ability to reduce a system’s information assurance.
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).

Term	Descriptions
Simple Network Management Protocol (SNMP)	A protocol used to configure, view, and in general, manage networked devices. Networked printers, switches, etc. often implement this protocol by default.
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. Social engineering attacks include non-technical intrusions into a GPE using information acquired through human interaction and rely on tricks that prey on an individual being unfamiliar with emerging technology and protocols.
Source Code	A text listing of commands to be compiled or assembled into an executable computer program.
Stateless Protocol	A communications scheme that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.
Switch	Connects devices on an 802.3 network. A switch forwards data to its destination by using the MAC address embedded in each packet.
System Administrator	The individual(s) responsible for maintaining the stable operation of the GPE (including software and hardware infrastructure and application software).
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.
Time Stamp	A record of the current value of the date and time which is added to a message at the time the message is created.
Transmission Control Protocol/Internet Protocol (TCP/IP)	The suite of communications protocols used to connect hosts on the Internet.
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
User Datagram Protocol (UDP)	A transport protocol that does not guarantee delivery. Thus, it is faster, but less reliable.
Version Control	The method by which evolving approved Critical System Components are verified to be operating in an approved state.
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.
Virus Scanner	Software used to prevent, detect and remove computer viruses, including malware, worms and Trojan horses.
Vulnerability	Software, hardware, or other weaknesses in a network or system that can provide a “door” to introducing a threat.
Wireless Access Point (WAP)	Provides network capabilities to wireless network devices. A WAP is often used to connect to a wired network, thereby acting as a link between wired and wireless portions of the network.
Wi-Fi	The standard wireless local area network (WLAN) technology for connecting computers and electronic devices to each other and/or to the internet.