GLI®

Gaming Security Framework

GLI-GSF-1

Gaming Information Security (GIS) Common Controls Audit

Version 1.0 DRAFT – Published April 19, 2024

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). This module of the GLI Gaming Security Framework, GLI-GSF-1, sets forth the gaming information security (GIS) common controls necessary for auditing a Gaming Organization's Gaming Information Security Management System (GISMS) to ensure effective management of security in a Gaming Organization's GPE. These GIS common controls apply to GPEs used for all forms of gaming, such as casino gaming, lottery, event wagering, and interactive gaming. Depending on the type of Gaming Organization, additional modules of the GLI-GSF may also apply. In addition, the GLI-GSF-*2 [To be released for comment in the near future]* will provide the guidance necessary to perform Gaming Technical Security (GTS) assessments of a Gaming Organization's GPE.

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

1.2. Gaming Production Environment (GPE)

A GPE refers to 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, including (but not limited to): casino gaming, lottery, event wagering, and interactive gaming. The GPE also encompasses the backend systems and infrastructure that interface and/or support gaming activities. Key characteristics of a GPE include:

a. Critical System Components: This includes the hardware and software platforms that support the execution of gaming activities, such as gaming devices, gaming tables, gaming systems, wagering systems, and interactive gaming systems or applications.

b. Transaction Processing: The GPE processes monetary transactions related to gaming activities, including wagers, payouts, deposits, withdrawals, and financial transactions with patrons.

c. Security Measures: Robust security measures are implemented to safeguard the security, integrity, confidentiality, and availability of critical system components, sensitive data, financial transactions, and patron information against unauthorized access, fraud, manipulation, and cyber threats.

d. Risk Management: The GPE employs risk management practices to identify, assess, mitigate, and monitor risks associated with gaming operations, including operational risks, financial risks, regulatory risks, and technological risks.

e. Continuous Operation: A GPE typically operates 24/7 to meet patron demand and maximize revenue generation. This requires high availability, reliability, and resilience of infrastructure and systems to minimize downtime and disruptions.

f. Monitoring and Control: Real-time monitoring, surveillance, and control mechanisms are in place to oversee gaming activities, detect anomalies, ensure compliance with rules and regulations, and respond promptly to GIS incidents, fraud, or other issues.

g. Regulatory Compliance: Compliance with gaming regulations, licensing requirements, and industry standards is essential in a GPE to ensure fair play, patron protection, responsible gaming practices, and adherence to legal and regulatory obligations.

1.3. Gaming Information Security Management System (GISMS)

A GISMS is a structured framework and set of processes designed to safeguard a Gaming Organization'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.

1.4. Framework Purpose

Ensuring the security and integrity of gaming activities is paramount for upholding public confidence and trust in the sector. Therefore, casinos, lotteries, event wagering operations, interactive gaming operations, and other Gaming Organizations 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.

2. GISMS AUDITS

2.1. Audit Overview

The GISMS 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, and availability of the information under the Gaming Organization's control are preserved. This approach relies heavily on layered security in order to reduce the risk to computer and network systems. The layered approach provides redundancy and reinforces the overall security model, as several layers of security must be breached before a critical data store is accessed.

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

2.2. Audit Methods

A GISMS audit uses a range of assessment methods including the following methods, the results of which are used to support the determination of GIS control effectiveness over time:

a. Interview: A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within a Gaming Organization to facilitate understanding, achieve clarification, or lead to the location of evidence.
b. Examine: A type of assessment method that is 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 that is 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 following are the high-level, suggested audit activities. The Appendix details the minimum GIS common control requirements in more granular detail. Users of this document are directed to the Appendix to ensure that no necessary GIS controls are overlooked. The GIS controls listed in the Appendix are not exhaustive and additional GIS controls may be included based on regulatory requirements and scope of the assessment.

2.3.1. Submitted Documentation Review

The ISF first evaluates the Gaming Organization's existing GIS controls by collecting and reviewing relevant documentation to better understand and assess pertinent aspects of the GPE in relation to overall GIS, and to determine if the documentation adequately complements the technical controls. An example of some of the documentation expected to be reviewed includes, but is not limited to:

a. GIS policy
b. User access
c. Development and testing procedures
d. Service Level Agreement
e. Policy on use of network services
f. Detection, prevention, and recovery controls to protect against malicious code

g. Data backup policy
h. Procedures in place so that media is disposed of securely and safely
i. Procedures for the handling and storage of information (to protect the information from unauthorized disclosure or misuse)
j. Change Management Program
k. Procedures for monitoring use of information processing facilities
l. Policies, operational plans, and procedures for teleworking activities
m. Policy on the use of cryptographic controls
n. Network diagram

2.3.2. Key Personnel Interviews

After collecting and reviewing relevant documentation, the ISF interviews key personnel (users, administrators, and management) to identify undocumented practices and gain feedback. As part of the interview process, the ISF discusses the actual practices in use and throughout the other phases of the assessment, the ISF identifies procedures in use based on the technical results of the assessment. This information allows the ISF to identify procedural gaps and to identify good practices that are not fully documented in the formal policies and procedures. Additionally, the ISF gauges the level of user awareness during the interviews to determine if users outside of the IT function have an appropriate level of understanding of GIS and their role in protecting information and other critical assets. The following key personnel responsible for establishing the GIS policy and applying shall be interviewed at a minimum.

a. Person with overall responsibility for the gaming operation
b. Compliance officer
c. Information security officer
d. Operational staff
e. Software developers

2.3.3. Administrative Controls Assessment

The ISF performs testing and evaluations to assess the effectiveness and adequacy of these administrative measures in mitigating risks and ensuring compliance with security requirements. This assessment typically addresses the following topics:

a. Policies, Standards and Guidelines
b. Organizational Security
c. Operations Management
d. Patch and Management Update
e. Monitoring System Access and Use
f. Change management procedures
g. Asset Classification and Control
h. Contingency Planning
i. GIS Incident Response

2.3.4. Technical Controls Assessment

The ISF performs testing and evaluations to assess the effectiveness and adequacy of these technical safeguards in mitigating risks and protecting sensitive data. This assessment typically addresses the following topics:

a. Infrastructure Design
b. Network Surveying / Penetration Testing
c. Network and Communications Security
d. Logical Access Controls
e. Operating Systems (OS) Security
f. Malicious Software Controls
g. Database Design and Configuration
h. Cryptographic Controls

i. System Monitoring
j. Reporting and Logging
k. System Development Controls

2.3.5. Physical and Environmental Controls Assessment

The ISF performs testing and evaluations to assess the effectiveness and adequacy of these controls in safeguarding against physical threats, environmental hazards, and unauthorized access to sensitive areas. This assessment typically addresses the following topics:

a. Location and Facility Security
b. Perimeter Security
c. Access Controls
d. Equipment Security
e. Intrusion Detection
f. Alarm Systems
g. Surveillance Systems
h. Heating, Ventilation and Air Conditioning
i. Power Systems
j. Power and Communications Cabling
k. Fire Detection and Suppression
l. Emergency Response

2.3.6. Risk Assessment

The ISF performs a risk assessment to identify issues of non-conformance to any applicable control, and any potential threats and vulnerabilities that may not be explicitly listed in the GLI-GSF but were observed during the audit and may constitute a risk.

2.4. Audit Frequency

2.4.1. Initial Audit

The Gaming Organization must have a GISMS audit performed by an ISF within ninety days of the Gaming Organization commencing gaming operations within that jurisdiction unless the regulatory body has advised otherwise. Any postponement of this audit as requested by the Gaming Organization, along with an updated audit schedule, shall be authorized by the regulatory body.

NOTE: It is recommended for regulatory bodies to allow flexibility for audit schedules for multi-jurisdictional Gaming Organizations to allow consolidation of audits for multiple jurisdictions to a common schedule.

2.4.2. Annual Audit

The Gaming Organization must, as a rule, have another GISMS audit performed by an ISF within twelve months of the previous GISMS audit unless the regulatory body has advised otherwise. Any postponement of this audit as requested by the Gaming Organization, along with an updated audit schedule, shall be authorized by the regulatory body.

NOTE: It is recommended for regulatory bodies to allow flexibility for audit schedules for multi-jurisdictional Gaming Organizations to allow consolidation of audits for multiple jurisdictions to a common schedule.

2.4.3. Additional Audits

Additional GISMS audits may be needed more frequently based on the critically of changes within the GPE, such as changes which may affect or provide access to sensitive data and/or critical system components.

2.5. GISMS Audit Reports

The results of a GISMS audit will identify for management those areas in the operations where improvement should be considered and recommend strategies for improving those areas. The GISMS audit report must be submitted to the regulatory body no later than sixty days after the GISMS audit has been completed. The GISMS audit report must include all the following:

a. The name and a brief background of the Gaming Organization, mentioning its business model and gaming activities offered or third-parties used, as well as the location, number of employees, website, actual certifications, high level description of the infrastructure including data center, etc.

b. The ISF's name, company affiliation, contact information, and qualifications and experience of the individuals who conducted the audit;

c. The date(s) of the audit, including the request date, the start date, the completion date, the report date, and the expiration date;

d. The scope of the audit, including:

    i. A high level overview of the work undertaken and the control environment operating;

    ii. The controls against which the audit was conducted;

    iii. The critical system components that were reviewed

    iv. How the critical system components were identified and if the audit included applications, networks, databases, and/or operating systems;

    v. An indication of any conditions of the audit, including the controls excluded from audit and the reasons for their exclusion;

e. The audit approach, including enquiry based questions, observation, evidence, key persons interviewed;

f. Evidence obtained during the audit to substantiate audit results, including:

    i. The documents that were reviewed, including version and dates, staff interviewed,.

    ii. The names, dates, and versions of documentation reviewed;

    iii. The names, roles, and locations of personnel interviewed;

    iv. The locations visited;

    v. The details of the walkthroughs performed;

    vi. The samples reviewed to verify compliance;

g. The results of the audit, indicating for each control its status as compliant, observation, minor non-conformity, or major non-conformity;

h. Findings, including:

    i. An explanation of the non-conformities identified;

    ii. Evidence that supports and describes the non-conformities;

    iii. Impact or potential impact of the non-conformities;

    iv. Recommended corrective actions to be taken to address existing non-conformities and make improvements;

i. The Gaming Organization's response to the findings and recommended corrective action, including resolution dates and responsible persons; and

j. Other relevant factors, such as whether the GISMS are compliant or have been audited against other requirements (e.g. ISO/IEC 27001, WLA-SCS, NIST-CSF, etc.)

2.6. Corrective Actions

If the ISF's GISMS audit report recommends corrective action, the Gaming Organization must provide the ISF and the regulatory body with a remediation plan and any risk mitigation plans which detail the Gaming Organization's actions and schedule to implement the corrective action.

a. Non-conformities shall be addressed through the Gaming Organization's corrective action process, including:

    i. Actions taken to determine the extent of and contain the specific non-conformance.

    ii. Root cause investigation to determine the most basic causes of the non-conformance.

    iii. Actions taken to correct the non-conformance and, in response to the root cause, to eliminate recurrence of the non-conformance.

b. Corrective actions to address the identified major non-conformities shall be carried out immediately and the ISF and the regulatory body shall be notified of the actions taken within thirty days, unless otherwise specified by the regulatory body. The ISF shall perform a follow up audit within ninety days to confirm the actions taken, evaluate their effectiveness, and determine whether the non-conformities have been resolved.

c. Corrective actions to address identified minor non-conformities shall be documented and sent by the Gaming Organization to the ISF and the regulatory body for review within thirty days, unless otherwise specified by the regulatory body. If the actions are deemed to be satisfactory, they will be followed up at the next scheduled audit.

d. Once corrective actions have been taken, the Gaming Organization will provide the ISF and the regulatory body with documentation evidencing completion.

e. The Gaming Organization must maintain corrective action records, including objective evidence, for at least three years, unless otherwise specified by the regulatory body.

2.7. Independent Security Firm (ISF)

The GISMS audit shall be carried out by individuals with sufficient qualifications, which means that the ISF shall hire sufficiently qualified, competent, and experienced individuals. These individuals shall:

a. Have relevant education background or in other ways provide relevant qualifications in assessing GPEs;

b. Obtain and maintain certifications sufficient to demonstrate proficiency and expertise as a qualified security professional by recognized certification boards, either nationally or internationally. The following certifications may demonstrate suitability to complete the GISMS audit:

   i. ISO/IEC 27001 Lead Auditor;
   ii. Certified Information Systems Auditor (CISA);
   iii. Certified Information Security Manager (CISM);
   iv. Certified Information Systems Security Professional (CISSP);

c. Have at least five years' experience performing GISMS audits within the gaming industry; and

d. Meet any other qualifications as prescribed by the regulatory body.

APPENDIX: GAMING INFORMATION SECURITY (GIS) CONTROLS

A. Adopted CIS Critical Security Controls

To establish a clear and reasonable baseline for GIS common controls, the GLI-GSF incorporates by reference the following controls of the Center for Internet Security (CIS) Critical Security Controls, Version 8, which must be met by each Gaming Organization (Enterprise).

NOTE: The entire CIS Critical Security Controls Document is available free of charge at www.cisecurity.org.

1	**Inventory and Control of Enterprise Assets**
1.1	Establish and Maintain Detailed Enterprise Asset Inventory
1.2	Address Unauthorized Assets
2	**Inventory and Control of Software Assets**
2.1	Establish and Maintain a Software Inventory
2.2	Ensure Authorized Software is Currently Supported
2.3	Address Unauthorized Software
3	**Data Protection**
3.1	Establish and Maintain a Data Management Process
3.2	Establish and Maintain a Data Inventory
3.4	Enforce Data Retention
3.5	Securely Dispose of Data
3.6	Encrypt Data on End-User Devices
3.7	Establish and Maintain a Data Classification Scheme
3.9	Encrypt Data on Removable Media
3.10	Encrypt Sensitive Data in Transit
3.11	Encrypt Sensitive Data at Rest
3.14	Log Sensitive Data Access
4	**Secure Configuration of Enterprise Assets and Software**
4.1	Establish and Maintain a Secure Configuration Process
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure
4.3	Configure Automatic Session Locking on Enterprise Assets
4.4	Implement and Manage a Firewall on Servers
4.6	Securely Manage Enterprise Assets and Software
4.7	Manage Default Accounts on Enterprise Assets and Software
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
4.9	Configure Trusted DNS Servers on Enterprise Assets
4.10	Enforce Automatic Device Lockout on Portable End-User Devices
5	**Account Management**
5.1	Establish and Maintain an Inventory of Accounts
5.2	Use Unique Passwords
5.3	Disable Dormant Accounts
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts
5.5	Establish and Maintain an Inventory of Service Accounts

5.6	Centralize Account Management
6	**Access Control Management**
6.1	Establish an Access Granting Process
6.2	Establish an Access Revoking Process
6.3	Require MFA for Externally-Exposed Applications
6.4	Require MFA for Remote Network Access
6.5	Require MFA for Administrative Access
6.7	Centralize Access Control
6.8	Define and Maintain Role-Based Access Control
7	**Continuous Vulnerability Management**
7.1	Establish and Maintain a Vulnerability Management Process
7.2	Establish and Maintain a Remediation Process
7.3	Perform Automated Operating System Patch Management
7.4	Perform Automated Application Patch Management
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
7.7	Remediate Detected Vulnerabilities
8	**Audit Log Management**
8.1	Establish and Maintain an Audit Log Management Process
8.2	Collect Audit Logs
8.3	Ensure Adequate Audit Log Storage
8.4	Standardize Time Synchronization
8.5	Collect Detailed Audit Logs
8.9	Centralize Audit Logs
8.10	Retain Audit Logs
8.11	Conduct Audit Log Reviews
8.12	Collect Service Provider Logs
9	**Email and Web Browser Protections**
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients
9.2	Use DNS Filtering Services
9.7	Deploy and Maintain Email Server Anti-Malware Protections
10	**Malware Defenses**
10.1	Deploy and Maintain Anti-Malware Software
10.2	Configure Automatic Anti-Malware Signature Updates
10.6	Centrally Manage Anti-Malware Software
10.7	Use Behavior-Based Anti-Malware Software
11	**Data Recovery**
11.1	Establish and Maintain a Data Recovery Process
11.2	Perform Automated Backups
11.3	Protect Recovery Data
11.4	Establish and Maintain an Isolated Instance of Recovery Data
11.5	Test Data Recovery

12	**Network Infrastructure Management**
12.1	Ensure Network Infrastructure is Up-to-Date
12.2	Establish and Maintain a Secure Network Architecture
12.3	Securely Manage Network Infrastructure
12.4	Establish and Maintain Architecture Diagram(s)
12.6	Use of Secure Network Management and Communication Protocols
13	**Network Monitoring and Defense**
13.1	Centralize Security Event Alerting
13.2	Deploy a Host-Based Intrusion Detection Solution
13.3	Deploy a Network Intrusion Detection Solution
13.4	Perform Traffic Filtering Between Network Segments
13.7	Deploy a Host-Based Intrusion Prevention Solution
13.8	Deploy a Network Intrusion Prevention Solution
13.9	Deploy Port-Level Access Control
13.10	Perform Application Layer Filtering
14	**Security Awareness and Skills Training**
14.1	Establish and Maintain a Security Awareness Program
14.2	Train Workforce Members to Recognize Social Engineering Attacks
14.3	Train Workforce Members on Authentication Best Practices
14.4	Train Workforce on Data Handling Best Practices
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents
14.9	Conduct Role-Specific Security Awareness and Skills Training
15	**Service Provider Management**
15.1	Establish and Maintain an Inventory of Service Providers
15.2	Establish and Maintain a Service Provider Management Policy
15.3	Classify Service Providers
15.4	Ensure Service Provider Contracts Include Security Requirements
15.5	Assess Service Providers
15.6	Monitor Service Providers
15.7	Securely Decommission Service Providers
16	**Application Software Security**
16.1	Establish and Maintain a Secure Application Development Process
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities
16.3	Perform Root Cause Analysis on Security Vulnerabilities
16.4	Establish and Manage an Inventory of Third-Party Software Components
16.5	Use Up-to-Date and Trusted Third-Party Software Components
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
16.8	Separate Production and Non-Production Systems
16.9	Train Developers in Application Security Concepts and Secure Coding
16.12	Implement Code-Level Security Checks
16.13	Conduct Application Penetration Testing
17	**Incident Response Management**

17.1	Designate Personnel to Manage Incident Handling
17.2	Establish and Maintain Contact Information for Reporting Security Incidents
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents
17.4	Establish and Maintain an Incident Response Process
17.5	Assign Key Roles and Responsibilities
17.6	Define Mechanisms for Communicating During Incident Response
17.7	Conduct Routine Incident Response Exercises
17.8	Conduct Post-Incident Reviews
17.9	Establish and Maintain Security Incident Thresholds
18	**Penetration Testing**
18.1	Establish and Maintain a Penetration Testing Program
18.2	Perform Periodic External Penetration Tests
18.3	Remediate Penetration Test Findings
18.4	Validate Security Measures
18.5	Perform Periodic Internal Penetration Tests

B. Additional GIS Common Controls

In addition to the CIS Critical Security Controls adopted previously, the following additional GIS common controls apply to GPEs used for all forms of gaming.

[To be included in the next comment period]

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.
Address Resolution Protocol (ARP)	The protocol used to translate IP addresses into MAC addresses to support communication on a wireless or wired local area network.
Administrative Controls	Policies, procedures, and guidelines implemented by a Gaming Organization to manage its GISMS.
Advanced Encryption Standards (AES)	A symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
Algorithm	A finite set of unambiguous instructions performed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired result. Algorithms are the basis for most computer programming.
Application	Computer software that is designed to help a user perform a specific task.
Audit Trail	A record showing who has accessed a system and what operations the user has performed 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
Backup	A copy of files and programs made to facilitate recovery if necessary.
Biometrics	A biological identification input, such as fingerprints or retina patterns.
Bridge	Divides networks to reduce overall network traffic. A bridge allows or prevents data from passing through it by reading the MAC address.
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.
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 System Component	Any hardware, software, 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 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. • 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,

Term	Descriptions
	components that control required system reporting, and database elements that affect gaming or system operations. • 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. • Corporate networks and systems that interface with the GPE and from which attackers could use to move laterally into the GPE, including corporate casinos' networks and online operators' corporate networks.
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 Name Service (DNS)	The globally distributed internet database which (amongst other things) maps machine names to IP numbers and vice-versa.
Domain	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
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.
Encryption Key	A cryptographic 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 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 organizational data, with the objective of ensuring acceptable levels of GIS risk.
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 confidentiality, integrity, 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 Organization's GPE
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.
Hash Algorithm	A function that converts a data string into an alpha-numeric string output of fixed length.

Term	Descriptions
Hypertext Transport Protocol (HTTP)	The underlying protocol used to define how messages are formatted and transmitted, and what actions servers and browsers shall take in response to various commands.
Hub	Connects devices on a twisted-pair network. A hub does not perform any tasks besides signal regeneration.
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 your system.
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.
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 cryptographic 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 cryptography.
Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.
Key Management	Activities involving the handling of cryptographic 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.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, 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.
Major Non-Conformity (MaNC)	A fundamental failing (systematic) has been identified that affects several 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-conformance; or • Any non-conformance 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-conformance 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. Until resolved, such an issue will normally mean the Gaming Organization is not compliant with the GLI-GSF.

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.
Minor Non-Conformity (MiNC)	A 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. A course of action to remedy this should be provided with an appropriate timeline.
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, pattern or answers to challenge 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, facial or voice recognition).
Network Communication Equipment (NCE)	One or more devices that controls data communication in a system including, but not limited to, cables, switches, bridges, hubs, routers, wireless access points, and telephones.
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 (OBS)	A policy is in place, but it is either not fully compliant with the GLI-GSF or the supporting evidence (or lack thereof) raised potential concerns. Any issues which are likely to become a non-conformance if not treated until the next audit are marked with this status.
Opportunities for Improvement (OFI)	These opportunities to help to improve the system as a whole or named processes. If certain aspects should be improved which generally comply with the requirements of the GLI-GSF though, then they are marked with this status.
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 patron. Examples include a legal name, date of birth, place of birth, social security number (or equivalent government identification number), driver's license number, passport number, residential address, phone number, email address, debit instrument number, credit card number, bank account number, 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.

Term	Descriptions
Protocol	A set of rules and conventions that specifies information exchange between devices, through a network or other media.
Remote Access	Any access from outside the system or system network including any access from other networks within the same site or venue.
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 shall have a valid Security Certificate.
Sensitive Data	Information such as PII, gaming data, validation numbers, authentication credentials, PINs, passwords, secure seeds and keys, and other data that shall be handled in a secure manner.
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 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.
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.

Term	Descriptions
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.
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).
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.
Wager	Any commitment of credits or money by the patron which has an impact on game outcome.
Wired Equivalent Protocol (WEP)	An easily broken and therefore deprecated algorithm to secure IEEE 802.11 wireless networks. It was originally intended to allow the same level of protection as a wired connection, but flaws were soon discovered after its adoption that made it barely better than no protection at all.
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.
Wi-Fi Protected Access (WPA)	The successor to WEP. Its authentication can be broken under certain circumstances, but sufficiently complex passphrases are secure enough for most uses.