GLI®

GAMING SECURITY FRAMEWORK

GLI-GSF-3

GAMING INFORMATION SECURITY (GIS) CONTROLS AUDIT – VENDOR CONTROLS

Version 1.0 – Published September 30, 2025

Contents

1. INTRODUCTION

1.1. General Statement

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

a. This module of the GLI Gaming Security Framework, GLI-GSF-3, establishes the additional Gaming Information Security (GIS) Controls to the GLI-GSF-1, which are necessary for specifically auditing a Vendor who integrates a business application or other ancillary solution into a Gaming Enterprise's GPE which does not directly affect regulated gaming components or activities.
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. Vendors and Gaming Enterprises

Ensuring the security of a GPE is a collective responsibility that spans across the multiple entities which make up the Gaming Enterprise who have a role in overseeing or the operation of a GPE or providing services integral to its function. For the purpose of this module, Vendors refer to Service Providers who integrate business applications and other ancillary solutions into a Gaming Enterprise's GPE which does not directly affect regulated gaming components or activities. For additional information, please refer to the "Gaming Enterprise and Sensitive Data Management Role" section of the GLI-GSF-1.

NOTE: Please note that, while reading and implementing the GLI-GSF-1's GIS Controls, the Vendor assumes the role of the "Gaming Enterprise" whereas the Gaming Enterprise assumes the role of the "Regulatory Body".

1.3. 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, gaming systems, software, and processes required to facilitate various forms of gaming, such as casino gaming, lottery, event wagering, and interactive gaming. The GPE also encompasses the backend systems, business applications, and infrastructure that interface and/or support 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 gaming activities is paramount for upholding public confidence and trust in the sector. Therefore, Gaming Enterprises and their Vendors must establish and uphold a clearly defined and documented framework to attain and preserve public trust in their operations. The goal is to align GIS in such a way that gaming operations can function as other eCommerce operations to ensure a safe and stable environment with the secure features of operations in parallel industries.

1.6. Security Standards and Guidelines Consulted

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

1.7. Adoption and Observance

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

2. VENDOR GIS (VGIS) CONTROLS AUDITS

2.1. Audit Overview

The VGIS Controls Audit is performed with the intent of identifying any actual or potential instances of non-compliance, vulnerabilities, or weaknesses, and assuring that the confidentiality, integrity, availability, and accountability of the information under the Gaming Enterprise's control are preserved when a Vendor's business application or other ancillary solution is integrated into the GPE. 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-3 is on specific information security controls for vendors to apply in addition to the common information security controls for gaming in GLI-GSF-1, other evaluation methods are discussed in supporting modules of the GLI-GSF.

2.2. Audit Methods

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

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

2.3. Audit Tasks

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

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

2.4. Audit Frequency

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

NOTE: The expectation is that a Vendor will only need to obtain one annual VGIS Controls Audit for each business application or other ancillary solution unless otherwise required by the Gaming Enterprise or Regulatory Body.

2.5. Audit Reports

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

2.6. Remediation

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

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

2.7. Independent Security Firm (ISF)

The VGIS 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 Gaming Enterprise or Regulatory Body, these individuals must meet the qualifications specified for an "Independent Security Firm (ISF)". in the GLI-GSF-1.

APPENDIX: VENDOR GAMING INFORMATION SECURITY (VGIS) CONTROLS

In addition to the GIS Controls specified in the GLI-GSF-1 for GIG1 Gaming Enterprises, the following additional GIS Controls apply to the integration of a Vendor's business application or other ancillary solution into GPEs used for any form of gaming. It may be possible that certain Common GIS Controls specified in GLI-GSF-1 for GIG1 Gaming Enterprises that relate specifically to regulated gaming are not applicable to a Vendor's business application or other ancillary solution.

VGIS-1	Vendor Organization
VGIS-1.1	**Vendor Privacy**
VGIS-1.1.1	The Vendor must demonstrate adherence to the principles of "privacy by design and by default" in the architecture, development, and operation of all products and services provided to the Gaming Enterprise.
VGIS-1.1.2	The Vendor must provide documented privacy impact assessments and design documentation demonstrating compliance with privacy by design principles.
VGIS-1.1.3	The Vendor must provide functionalities and documentation supporting the Gaming Enterprise's compliance with relevant data privacy laws (e.g., GDPR, CCPA), including consent management and data subject rights fulfillment.
VGIS-1.2	**Responsible Disclosure**
VGIS-1.2.1	The Vendor must disclose any security vulnerabilities of their products and/or services to all Gaming Enterprises who have purchased them.
VGIS-1.2.2	The Vendor must establish a policy and associated process for dealing with responsible disclosures, which identifies where reports should be made and how rapidly they will be assessed and acted on, if necessary.
VGIS-1.3	**Security Incident Collaboration and Response**
VGIS-1.3.1	The Vendor must have established and documented processes for effective collaboration with all impacted Gaming Enterprises during any security incident that affects the business applications and other ancillary solutions provided.
VGIS-1.3.2	The Vendor must notify affected Gaming Enterprises without undue delay upon identification and confirmation of a security incident.
VGIS-1.3.3	The Vendor must have established processes for collaborating with involved Gaming Enterprises during security incidents that affect the provided service. This includes timely notification, information sharing, and coordinated response and recovery efforts.
VGIS-1.3.4	The Vendor must provide timely and accurate updates, including: a. Nature and scope of the incident; b. Systems or data impacted; c. Known or suspected cause; d. Mitigation actions underway; and e. Recommended patron actions.
VGIS-1.3.5	The Vendor must actively coordinate with the Gaming Enterprise to: a. Contain the incident; b. Restore affected services; c. Support forensic investigation if required; and d. Prevent recurrence through corrective actions.
VGIS-2	**Accounts and Privilege Management**
VGIS-2.1	**Accounts and Privilege Activity Logs**
VGIS-2.1.1	The Vendor must ensure that all account-related activities or privilege-related activities, including creation, modification, and deletion or removal of accounts and privileges, are fully logged and monitored for the purpose of supporting periodic audit and investigations.
VGIS-2.1.2	In cases where account-related activities or privilege-related activities are initiated by the Vendor, the system must: a. Generate real-time alerts to the Gaming Enterprise's designated security contact(s); b. Generate real-time event logs compliant with required log transfer and accessibility controls; c. Record detailed logs including the time stamp, initiating user or system, nature of the change, and affected account(s); and d. Ensure all logs are tamper-evident and retained in accordance with the Gaming Enterprise's logging and audit retention policies.

VGIS-2.2	Accounts and Privilege Control
VGIS-2.2.1	The Vendor is obligated to provide the Gaming Enterprise with the ability to enable, disable, and delete user accounts for access to the Vendor's business applications and other ancillary solutions, and to grant and revoke privileges, at the Gaming Enterprise's discretion.
VGIS-2.2.2	The functionality to enable or disable user accounts and to grant and revoke privileges must be available to the Gaming Enterprise at all times, ensuring they can manage access and privileges based on operational, security, or compliance requirements without Vendor intervention or delay.
VGIS-2.2.3	When requested, the Vendor must maintain the technical capability to integrate with the Gaming Enterprise's automated systems for real-time account activation and deactivation through industry standard protocols compatible with generally available provisioning and deprovisioning tools.
VGIS-2.3	Elevated Accounts
VGIS-2.3.1	A Vendor requesting elevated access to a Gaming Enterprise's GPE must follow a real-time approval process.
VGIS-2.3.2	The Vendor must not access the Gaming Enterprise's GPE directly without prior authorization.
VGIS-2.3.3	All access must adhere to the Gaming Enterprise's defined approval procedures or utilize pre-approved methods that ensure the Gaming Enterprise retains full control, including the ability to revoke access at any time.
VGIS-2.3.4	The Vendor must ensure all access attempts and activities within the Gaming Enterprise's GPE are logged in detail and made available upon request and transferred to the Gaming Enterprise.
VGIS-2.3.5	In cases where cloud-based Software-as-a-Service (SaaS) solutions are used, the Vendor must ensure that contractual agreements include provisions for third-party audits to verify compliance with industry best practices.
VGIS-2.4	Role-Based Access Controls (RBAC)
VGIS-2.4.1	RBAC must be implemented and be granular enough to support segmented administrative functions (e.g. user provisioning should not require full admin rights).
VGIS-2.4.2	The Gaming Enterprise must have the technical capability to configure permissions by role, which then can be applied to groups or users.
VGIS-2.4.3	Default roles are acceptable where the permissions to the role are visible by the Gaming Enterprise for audit purposes. It is acceptable to display "All" for the top-level admin role (e.g. superuser, global admin).
VGIS-2.5	Account and Privilege Events
VGIS-2.5.1	The Vendor must ensure that the following events are thoroughly logged. This level of detail is required to support auditing, forensic analysis, and compliance monitoring, and fills the gap when point-in-time (monthly, quarterly, etc.) permission audits are performed. a. All account-related events. For example, if a system is configured to lock an account after three failed login attempts, the logs must reflect all related activity, there should be three distinct failed login events logged, followed by a separate account lockout event logged, totaling four logged entries; and b. All privilege-related events. For example, if a user grants permissions to a role and subsequently removes that permission, there should be two events logged showing which permissions were modified by role.
VGIS-2.6	User Authentication
VGIS-2.6.1	When requested, the Vendor must maintain the technical capability to: a. Integrate with the Gaming Enterprise's single-sign on systems through industry standard protocols compatible with generally available systems for single sign-on (SSO); and b. Enforce multi-factor authentication (MFA) through sufficiently robust industry standard methods (push notification, TOTP, hardware token - not SMS).
VGIS-2.6.2	Every successful and failed attempt to change an account password, PIN, or other authentication credential must be logged and contain the following: a. Date and time of event; b. Hostname or IP address of the client where the event was initiated. Note that in some cases, correlating "successful logon" events may serve to meet this control; c. Hostname, IP address, or other unique identifier of system where account change occurred. Note that in certain load-balanced scenarios, typically on-premises, the server where the change occurred must be identifiable. This control does not apply to third-party SaaS systems where the system or tenant is identifiable through other methods; d. Outcome of event (Successful or Failed);

	e. Unique identifier of target account (the account the password change applies to); and f. Unique identifier of initiated account (the account that changed the password of the target account).
VGIS-3	**Log Transfer and Accessibility**
VGIS-3.1	**Log Generation and Retention**
VGIS-3.1.1	Where logs are generated by the Vendor's business applications or other ancillary solutions, the Vendor must ensure these logs are securely retained and readily accessible to the Gaming Enterprise upon request to support forensic investigation or audit requirements.
VGIS-3.2	**Transfer Capability and Integrity**
VGIS-3.2.1	When requested, the Vendor must maintain the technical capability to transfer logs to the Gaming Enterprise's centralized logging system or an equivalent solution, in a timely manner and in an industry standard format compatible with generally available monitoring and incident response tools.
VGIS-3.2.2	All log transfers must be conducted over secure channels using industry-standard encryption protocols to maintain the confidentiality and integrity of the data in transit.
VGIS-3.2.3	Transferred logs must be complete, unaltered, and in a structured format that preserves time stamp integrity, source system identifiers, and event details necessary for traceability and audit.
VGIS-3.2.4	Transferred logs must be reconcilable against a native system report to support integrity checks for sampling or full reperformance testing.
VGIS-4	**Supply Chain Management**
VGIS-4.1	**Supply Chain Risk Management (SCRM) Plan**
VGIS-4.1.1	The Vendor must implement and maintain a current, comprehensive, and documented Supply Chain Risk Management (SCRM) Plan to ensure the integrity, security, and reliability of all systems, components, and services provided to a Gaming Enterprise under an agreement.
VGIS-4.1.2	The SCRM Plan must outline the policies, procedures, roles, responsibilities, and processes used to identify, assess, mitigate, and monitor supply chain risks throughout the lifecycle of the product or service.
VGIS-4.1.3	The Vendor must establish, maintain, and periodically review formal policies and procedures that support the execution of the SCRM Plan. These documents must be made available to the Gaming Enterprise upon request for the purposes of oversight and compliance verification.
VGIS-4.2	**Supply Chain Risk Assessment and Review**
VGIS-4.2.1	The Vendor must perform regular risk assessments and reviews of all supply chain entities, including subcontractors, service providers, and other external suppliers.
VGIS-4.2.2	These risk assessments and reviews performed by the Vendor must evaluate the risks associated with each supplier or contractor and the specific system, system component, or service they provide.
VGIS-4.2.3	The Vendor must take appropriate actions to mitigate identified risks in accordance with industry best practices and contractual requirements.
VGIS-4.3	**Anti-Counterfeit Policies and Procedures**
VGIS-4.3.1	The Vendor must develop, document, and implement anti-counterfeit policies and procedures designed to detect, prevent, and respond to the introduction of counterfeit components into the system.
VGIS-4.3.2	The implemented anti-counterfeit policies and procedures must include methods for component verification, supplier validation, incident response, and reporting.
VGIS-4.4	**Supply Chain Mapping and Analysis**
VGIS-4.4.1	The Vendor must perform a comprehensive mapping and analysis of the software supply chain, including identifying and documenting all software components (proprietary, open-source, and third-party), their sources, dependencies, and relationships.
VGIS-4.4.2	The Vendor must ensure transparency and traceability across the supply chain and maintain this mapping throughout the lifecycle of the system, component, or service.
VGIS-5	**Secure Software Development & Deployment**
VGIS-5.1	**Controlled Deployments**
VGIS-5.1.2	The Vendor must not perform any automated software deployments to the Gaming Enterprise's GPE without prior scheduling, explicit approval, and logging by the Gaming Enterprise.
VGIS-5.1.3	All deployment events must be traceable and subject to the Gaming Enterprise's change management program.

VGIS-5.2	**Secure Coding & Continuous Integration/Continuous Deployment Pipelines**
VGIS-5.2.1	The Vendor must follow secure coding standards (e.g., OWASP), which must be consistently applied throughout the development process.
VGIS-5.2.2	The Vendor must conduct rigorous code reviews as well as integrate static and dynamic code analysis tools into the CI/CD (Continuous Integration/Continuous Deployment) pipeline to detect and remediate vulnerabilities.
VGIS-5.2.3	The Vendor's CI/CD pipelines must be secured with robust controls, including: a. Access control and audit logging for code repositories; b. Secure build environments and artifact management; c. Deployment gating and change management policies; and d. Protection against unauthorized modifications to pipeline logic.
VGIS-5.3	**Software Integrity**
VGIS-5.3.1	All software releases must be digitally signed by the Vendor using cryptographic techniques to ensure authenticity, prevent tampering, and enable verification of origin.
VGIS-5.3.2	The Vendor must implement checksum and cryptographic hash validation mechanisms during the packaging, distribution, and deployment phases to ensure the integrity of software components.
VGIS-5.3.3	The Vendor must employ integrity verification tools to detect unauthorized modifications to software components. Any deviation from the expected state must trigger alerts and incident response procedures.
VGIS-5.3.4	The Vendor must support or directly implement application whitelisting to ensure only authorized and validated software components are executed within the GPE.
VGIS-5.4	**Function Isolation**
VGIS-5.4.1	Security functions must be logically and physically isolated from non-security functions, ensuring that sensitive operations (e.g., authentication, cryptographic processes, auditing) are protected from compromise.
VGIS-5.4.2	The Vendor must ensure clear separation between user-facing functionality (e.g., user interfaces, gaming interaction) and system management functionality (e.g., administrative tools, configuration panels) to prevent privilege misuse and reduce attack surfaces.
VGIS-5.5	**Security Requirements and Threat Modeling**
VGIS-5.5.1	Security requirements must be defined by the Vendor at the outset, alongside functional requirements. This includes compliance with relevant regulations (e.g., data privacy laws), adherence to industry best practices, and internal security policies.
VGIS-5.5.2	Threat modeling must be performed by the Vendor at the earliest stages of development and maintained throughout the software lifecycle. The Vendor must identify and evaluate potential attack vectors and implement appropriate design mitigations to address them.
VGIS-5.6	**Secure Design Principles and Configuration Management**
VGIS-5.6.1	The Vendor must apply recognized secure design principles, including but not limited to: a. Principle of Least Privilege: Access rights must be limited to the minimum necessary for function. b. Defense in Depth: Multiple layers of controls must be implemented to mitigate risk at various levels. c. Fail Securely: Software must handle failures in a secure and controlled manner without exposing sensitive data or functionality. d. Simplicity in Design: Software design must minimize complexity to reduce the risk of vulnerabilities and facilitate maintainability.
VGIS-5.6.2	The Vendor must apply secure configuration management across all deployment environments, including development, testing, staging, and production. These configurations must be managed, version-controlled, and regularly reviewed for compliance with security standards.
VGIS-5.7	**Firewall Configuration and Connectivity**
VGIS-5.7.1	The Vendor must ensure and support operation of the product behind a host-based or network-based firewall.
VGIS-5.7.2	For services listening for inbound connections, the Vendor must supply details for destination port, protocol, and application (e.g. HTTP, SSL, MS-SQL) to be allowed through the Gaming Enterprise's firewall. Details for the source must be provided as a guideline (e.g. Internet clients with web browser, Internal clients with software developed by the Vendor).

VGIS-5.7.3	For software initiating outbound connections, the Vendor must supply details for the destination port, protocol, and application (e.g. HTTP, SSL, MS-SQL) to be allowed through the Gaming Enterprise's firewall. Details for the destination must be provided as a guideline (e.g. FQDN or IP range of Vendor's cloud/SaaS environment, location of installed listening service provided by Vendor and deployed in the Gaming Enterprise's GPE). Overly broad destination IP ranges where other services may reside are not acceptable (e.g. shared IP ranges in a cloud environment such as AWS, Azure, GCP).
VGIS-6	**Vendor Gaming Technical Security (GTS) Testing**
VGIS-6.1	**Testing Methodology**
VGIS-6.1.1	The Vendor must conduct Vendor GTS Testing in accordance with the methodologies and requirements outlined in the GLI-GSF-2.
VGIS-6.1.2	The Vendor GTS Testing must include the evaluation of the business applications and/or ancillary services for vulnerabilities, misconfigurations, and unauthorized access paths.
VGIS-6.2	**Risk-Based Scope Adjustment**
VGIS-6.2.1	The scope of Vendor GTS Testing may be adjusted based on the size, context, and nature of the business applications and/or ancillary services being integrated into the Gaming Enterprise’s GPE.
VGIS-6.2.2	Adjustments to the scope must consider the potential impact, security implications, and level of risk the business applications and/or ancillary services presents to the integrity and operation of the GPE.
VGIS-6.2.3	Any modifications to scope of Vendor GTS Testing require prior review and approval by the Gaming Enterprise.
VGIS-6.2.4	The Vendor must document the justification for all scope adjustments and maintain a verifiable record of approvals granted by the Gaming Enterprise.

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.
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.
Availability	Ensuring timely and reliable access to and use of information.
Business Applications	Applications operating as a shared service for users to collect, process, maintain, use, share, disseminate, or dispose of sensitive data within the GPE for compliance auditing and GIS incident response purposes.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical System Component	Any hardware, software, critical control programs, communications technology, other equipment or components implemented in a GPE to allow patron participation in gaming, and whose failure or compromise can lead to loss of patron entitlements, government revenue or unauthorized access to data used for generating reports for the Regulatory Body. Examples of Critical System Components include, but are not limited to: • Components which record, store, process, share, transmit, or retrieve sensitive data. • Components that could impact the security of sensitive data or the GPE. • Components which generate, transmit, or process random numbers used to determine the outcome of games and events. • Components which store results or the current state of a patron's game, wager, or available funds. • Points of entry to and exit from the above components, including other systems which communicate directly with Critical System Components. • Communications technology and networks which transmit sensitive data, including network communication equipment (NCE) and network security controls. • Components that provide security services, including authentication servers, access control servers, security information and event management (SIEM) systems, physical security systems, surveillance systems, multi-factor authentication (MFA) systems, anti-malware/anti-virus systems. • Components that facilitate segmentation, including internal network security controls. • Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. • Cloud infrastructure and components, both external and on premises, and including instantiations of containers or images, virtual private clouds, cloud-based identity and access management, components residing on premises or in the cloud, service meshes with containerized applications, and container orchestration tools. • Server types including web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name Service (DNS).

Term	Descriptions
	• 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.
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.
Gaming Enterprise	An operator, and any suppliers, manufacturers, vendors, service providers, and/or other entities who have a role in overseeing the operation of a GPE, or providing services integral to its function, including the management of sensitive data.
Gaming Information Security (GIS)	Protecting sensitive data and Critical System Components from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, availability, and accountability.
Gaming Information Security Management System (GISMS)	A defined, documented management system that consists of a set of policies, processes, and systems to manage risks to a Gaming Enterprise's sensitive data, assets, and Critical System Components within a GPE, with the objective of ensuring acceptable levels of GIS risk.
Gaming Production Environment (GPE)	The operational setting where gaming activities and related services are conducted, managed, and delivered to patrons in a live or real-time manner. It encompasses the physical and virtual infrastructure, gaming systems, software, and processes required to facilitate various forms of gaming and/or manage sensitive data, as well as the backend systems and infrastructure that interface and/or support gaming activities.
GIS Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, availability, or accountability of a GPE or the sensitive data the GPE processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Examples of reportable GIS incidents include, but are not limited to: • Unauthorized access to sensitive data or Critical System Components. • Malicious code execution or ransomware infection within the GPE. • Loss, theft, or unauthorized disclosure of PII. • System outages or disruptions affecting the integrity or availability of gaming operations for a defined period (e.g., more than 15 minutes). • Detection of tampering, manipulation, or attempted compromise of gaming software or hardware. • Repeated or systemic failed login attempts indicative of a brute-force attack. • Compromise or misuse of administrative credentials or security certificates. • Security configuration changes that were made outside of authorized change management processes.
GIS Incident Response Plan	The documentation of a predetermined set of instructions or procedures when a malicious cyberattack is encountered against a Gaming Enterprise's GPE.

Term	Descriptions
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Layered Security	A defense approach that uses multiple independent protections across a system, like firewalls, authentication, encryption, and monitoring, so that an attacker must bypass several layers before accessing sensitive data or Critical System Components.
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).
Protocol	A set of rules and conventions that specify information exchange between devices, through a network or other media.
Regulatory Body	The governmental body or equivalent which regulates or controls the operations of gaming.
Risk	The likelihood of a threat being successful in its attack against a network or system within the GPE.
Risk Assessment	Identifying, analyzing, and prioritizing threats and vulnerabilities to a Gaming Enterprise's operations or assets, or to individuals or other entities, resulting from impairment of the confidentiality, integrity, availability, and accountability of sensitive data or the reliability, security, or capacity of the GPE.

Sensitive Data	Information that needs to be handled in a secure manner, including but not limited to, as applicable:
	• Audit logs and system databases recording information used to determine outcome, payment, redemption, and the tracking of patron information;
	• Accounting and significant event information related to the Critical System Components of the GPE;
	• RNG seeds and any other information which affects outcomes of games and wagers;
	• Encryption keys, where the implementation chosen requires transmission of keys;
	• Validation numbers associated with patron accounts, wagering instruments, and any other gaming transactions;
	• Transfers of funds to and from patron accounts, electronic payment accounts, and for the purposes of gaming;
	• Software packages within the GPE;
	• 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

Term	Descriptions
	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.
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.
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
Vendors	Service Providers that integrate business applications and other ancillary solutions into a Gaming Enterprise’s GPE which does not directly affect regulated gaming components or activities.