GLI®

GAMING SECURITY FRAMEWORK

GLI-GSF-2

GAMING TECHNICAL SECURITY (GTS) ASSESSMENT

Version 1.0 DRAFT – Published October 4, 2024

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-2 establishes a benchmark for conducting Gaming Technical Security (GTS) assessments of a Gaming Enterprise's GPE.
b. These GTS tests apply to GPEs used for all forms of gaming, such as casino gaming, lottery, event wagering, and interactive gaming.
c. This module may be used alongside the GLI-GSF-1, provides the gaming information security (GIS) common controls necessary for auditing a Gaming Enterprise's Gaming Information Security Management System (GISMS)
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, which at a minimum consists of the following, as applicable:

a. Audit logs and system databases recording information used to determine outcome, payment, redemption, and the tracking of patron information;
b. Accounting and significant event information related to the Critical System Components of the GPE;
c. RNG seeds and any other information which affects outcomes of games and wagers;
d. Encryption keys, where the implementation chosen requires transmission of keys;
e. Validation numbers associated with patron accounts, wagering instruments, and any other gaming transactions;
f. Transfers of funds to and from patron accounts, electronic payment accounts, and for the purposes of gaming;
g. Software packages within the GPE;
h. Any location data related to employee or patron activity (e.g. account management, online gaming, etc.);
i. Any of the following information recorded for any employee or patron:
    i. Government identification number (social security number, taxpayer identification number, passport number, or equivalent);
    ii. Personal financial information (credit or debit instrument numbers, bank account numbers, etc.);
    iii. Authentication credentials in relation to any user account or patron account;
    iv. Any other personally identifiable information (PII) which needs to be kept confidential; and
j. Any other data deemed sensitive by the regulatory body or the Gaming Enterprise.

NOTE: This document is not intended to define which entities are responsible for meeting each control as detailed herein. 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 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, 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 include:

a. Critical System Components: This includes the network devices, servers, computing devices, virtual components, hardware, and software platforms that support the execution of gaming activities, such as gaming devices, gaming tables, gaming systems, lottery systems, event wagering systems, and interactive gaming systems or applications.
b. Cryptographic Modules: Cryptographic modules used within the GPE are responsible for cryptographic functions, including the encryption and decryption of sensitive data, using algorithms which meet current industry accepted standards, such as ISO/IEC 19790, FIPS 140-2, or equivalent.
c. Transaction Processing: The GPE processes monetary transactions related to gaming activities, including wagers, payouts, deposits, withdrawals, and financial transactions with patrons.
d. Security Measures: Robust security measures are implemented to safeguard the integrity, confidentiality, and availability of Critical System Components, sensitive data, financial transactions, and patron information against unauthorized access, fraud, manipulation, and cyber threats.
e. 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.
f. 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.
g. 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.
h. 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.

1.4. 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, casinos, lotteries, event wagering operations, interactive gaming operations, and other Gaming Enterprises 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

The GLI-GSF was based on commonly used security standards and guidelines that provide an industry-accepted foundation developing effective GTS 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.

2. GTS ASSESSMENTS

2.1. Assessment Overview

The GTS assessment 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 approach relies heavily on layered security 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 sensitive data store is accessed.

NOTE: The focus of the GTS guidance detailed in the GLI-GSF-2 is on technical security tests for gaming, other evaluation methods are discussed in supporting modules of the GLI-GSF.

2.2. Assessment Methods

A GTS assessment uses a range of assessment methods including the following methods, the results of which are used to support the determination of a GPE's security:

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

2.3. Assessment Tasks

The following are the high-level, suggested assessment activities. The Appendix details the minimum GTS test requirements in more granular detail. Users of this document are directed to the Appendix to ensure that no necessary GTS tests are overlooked. The GTS tests listed in the Appendix are not exhaustive and additional GTS tests may be included based on regulatory requirements and scope of the assessment. These assessments must encompass more than automated scans and incorporate manual penetration testing techniques.

2.3.1. Vulnerability Assessment

The ISF performs a vulnerability assessment of the Gaming Enterprise's systems, internet websites, mobile applications, internal, external, and wireless networks with the intent of identifying vulnerabilities or potential vulnerabilities of devices, systems, and applications transferring, storing, or processing sensitive data connected to or present on the networks. Vulnerability assessments include identifying and passively quantifying potential risks within the GPE.

2.3.2. Penetration Testing

The ISF performs a penetration test of the Gaming Enterprise's systems, internet websites, mobile applications, and internal, external, and wireless networks to confirm if identified vulnerabilities of devices, systems, and applications are susceptible to compromise. Simply running a vulnerability scan and providing those results is not sufficient to comply with penetration testing requirements. There must be some form, of manual verification and/or exploitation. Penetration tests include:

a. Evaluating the security of both external and internal environments of the GPE.
b. Identifying weaknesses that could be exploited by attackers to gain unauthorized access, disrupt operations, or exfiltrate sensitive data.
c. Simulating potential attack scenarios to understand the impact of vulnerabilities on the GPE's security posture.
d. Validating the findings from vulnerability assessments through manual testing techniques.

2.3.3. Risk Assessments

The ISF performs a risk assessment to identify potential threats and vulnerabilities, and non-conformities to any applicable control that may not be explicitly listed in the GLI-GSF but were observed during the audit and may constitute a risk. The ISF must use an appropriate scoring system for gaming security (e.g. CVSS, ISO/IEC 31010, etc.) for assigning severity scores to threats, vulnerabilities, and non-conformities, allowing prioritization of responses and resources according to the level of severity. The scoring system used by the ISF must be identified in the assessment report.

2.4. Assessment Frequency

2.4.1. Initial Assessment

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

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

2.4.2. Annual Assessment

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

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

2.4.3. Additional Assessments

The Gaming Enterprise must, as a rule, have additional GTS assessments performed by an ISF after any critical changes within the GPE, such as infrastructure or application upgrades and modifications, or the installation of new Critical System Components. The determination of what constitutes a "critical" change is based on the Gaming Enterprise's risk assessment process, the specific configuration of the GPE, and the requirements of the regulatory body. However, any change that could affect the security of the GPE or allow access to sensitive data and/or Critical System Components may be deemed "critical" by the Gaming Enterprise. These GTS assessments ensure that the controls expected to be in place continue to function effectively following the upgrade or modification.

2.5. Assessment Reports

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

a. Executive Summary:
   i. The Gaming Enterprise’s name and contact information;
   ii. A brief overview of the Gaming Enterprise’s business model, gaming activities offered, Service Providers utilized, location, number of employees, website, certifications, and a high-level description of the IT infrastructure (including data centers, cloud services, etc.)
b. Assessment Details:
   i. The ISF’s name, company affiliation, contact information, and qualifications and experience of the individuals who conducted the assessment;
   ii. The date(s) of the assessment, including the request date, the start date, the completion date, and the report date;

c. Scope of the Assessment:
   i. A high-level overview of the testing performed, specifying the environments (e.g., development, production) and the types of systems tested (e.g., web applications, networks, databases, operating systems).
   ii. Identification of Critical System Components and assets reviewed, detailing how these components and assets were selected as part of the assessment.
   iii. Specific tools and techniques used during the GTS assessment, including software names, versions, and official websites for the tools employed.
d. Methodology:
   i. A detailed description of the penetration testing methodology or vulnerability assessment framework applied (e.g., OWASP, OSSTMM).
   ii. Any limitations or exclusions in the assessment, with justifications (e.g., certain systems were out of scope due to business requirements).
e. Evidence Collected:
   i. Documentation reviewed, including the names, dates, and versions.
   ii. Personnel interviewed, with roles, locations, names, dates, and versions of interviews.
   iii. Screenshots, logs, or other evidence that clearly illustrate the vulnerabilities identified, including commands and tools used to discover these issues.
   iv. Sampling techniques used to verify the security posture, including the size and nature of the sample.
f. Findings and Results:
   i. A summary of the vulnerabilities discovered, categorized by severity (e.g., critical, high, medium, low).
   ii. A detailed explanation of each vulnerability, supported by evidence (e.g., screenshots, logs).
   iii. An assessment of the potential impact or risk associated with each identified vulnerability, considering the gaming enterprise's specific environment.
   iv. Recommended remediation steps for each identified vulnerability, with priority levels and suggested timelines for mitigation.

2.6. Remediation

If the ISF's GTS assessment report recommends remediation, the Gaming Enterprise must provide the ISF and 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.

a. Vulnerabilities must be addressed through the Gaming Enterprise's remediation process, including:
   i. Actions taken to determine the extent of and contain the specific vulnerability.
   ii. Root cause investigation to determine the most basic causes of the vulnerability.
   iii. Actions taken to correct the vulnerability and, in response to the root cause, to eliminate recurrence of the vulnerability.
b. Remediation steps to address the identified major vulnerabilities must be carried out immediately and the ISF and the regulatory body must be notified of the actions taken within thirty days, unless otherwise specified by the regulatory body. Unless otherwise specified by the regulatory body, the ISF must perform a follow up assessment within a reasonable timeframe to confirm the actions taken, evaluate their effectiveness, and determine whether the vulnerabilities have been resolved.
c. Remediation steps to address identified minor vulnerabilities must be documented and sent by the Gaming Enterprise to the ISF and the regulatory body for review within thirty days, unless otherwise specified by the regulatory body. If the actions are deemed satisfactory, they will be followed up at the next scheduled assessment.
d. Once remediation steps have been taken, the Gaming Enterprise will provide the ISF and the regulatory body with documentation evidencing completion.
e. The Gaming Enterprise must maintain remediation records, including objective evidence, for at least five years, unless otherwise specified by the regulatory body.

2.7. Independent Security Firm (ISF)

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

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 GTS assessment:
    i. Offensive Security Certified Professional (OSCP)
    ii. Certified Ethical Hacker (CEH)
    iii. Global Information Assurance Certification (GIAC) Certifications (e.g., GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), or GIAC Exploit Researcher and Advanced Penetration Tester (GXPN))
    iv. Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) certification
    v. Tiger Scheme: Senior Security Tester, Qualified Security Tester
    vi. Approved Scanning Vendor (ASV)
c. Have at least five years' experience performing GTS assessments within the gaming industry or, where acceptable to the regulatory body, other relevant security testing experience of a similar industry; and
d. Meet any other qualifications as prescribed by the regulatory body.

NOTE: Nothing herein is intended to prohibit the regulatory body staff from acting as an ISF, provided they are independent from the Gaming Enterprise being assessed.

3. RECURRING VULNERABILITY SCANS

3.1. Cadence of Scans

Unless otherwise specified by the regulatory body, internal and external network vulnerability scans must be run at least quarterly and after any significant change to the GPE. Testing procedures must verify that four quarterly internal and external scans took place in the past twelve months.

NOTE: It is recommended for regulatory bodies to allow flexibility for vulnerability scans for multi-jurisdictional Gaming Enterprises to allow consolidation of vulnerability scans for multiple jurisdictions to a common schedule.

3.2. Scanner Requirements

Vulnerability scanners must be used to test for the vulnerabilities of internal network devices, applications, and network perimeter defenses, as well as adherence to security plan and standards. Vulnerability scanners must have the ability to handle the following minimum tasks:

a. Non-Disruptive: The scanner must be configured to avoid disruptive testing methods that could cause system crashes, reboots, or interfere with network services such as Domain Name Service (DNS), routing, or switching. Additionally, the installation of software (e.g., rootkits) should only occur if it is a pre-approved part of the scanning solution.
b. Host Discovery: The scanner must accurately identify live systems, including those that do not respond to standard Internet Control Message Protocol (ICMP) echo ("ping") requests.
c. Service Discovery: The scanner must perform thorough port scanning on all Transmission Control Protocol (TCP) ports and common User Datagram Protocol (UDP) ports, ensuring comprehensive coverage of services like authentication protocols, database servers, and other critical infrastructure components.
d. Operating System and Service Fingerprinting: The scanner should accurately identify operating systems and service versions to help prioritize remediation efforts effectively.
e. Platform Independence: The scanning solution must be compatible with all commonly used platforms, ensuring broad applicability.
f. Accuracy: The scanner must report both confirmed and potential vulnerabilities with a high level of certainty, ensuring that even potential risks are accounted for in compliance determinations.
g. Load Balancer Consideration: In environments using load balancers, the scanner must account for potential configuration inconsistencies and ensure that all relevant IP addresses are adequately scanned.

h. Component-Specific Requirements: The scanner must be capable of detecting vulnerabilities across various components, ensuring comprehensive coverage of all potential security risks. Key components include:
   i. Firewalls and Routers: Scan for vulnerabilities and configuration issues that could compromise network security.
   ii. Operating Systems: Detect known exploits and ensure systems are adequately patched.
   iii. Database Servers: Identify any open access from the Internet and detect known vulnerabilities.
   iv. Web Servers: Test for vulnerabilities and configuration issues, including directory browsing.
   v. Application Servers: Detect the presence of vulnerabilities in application servers and their configurations.
   vi. Common Web Scripts: Identify vulnerabilities in scripts like CGI, ASP, and PHP.
   vii. Built-in Accounts: Detect default accounts and passwords, reporting any such vulnerabilities.
   viii. DNS Servers: Detect vulnerabilities, including issues with DNS zone transfers.
   ix. Mail Servers: Identify vulnerabilities specific to mail server configurations.
   x. Virtualization Components: Detect vulnerabilities in virtual hosts, machines, and hypervisors.
   xi. Web Applications: Detect vulnerabilities such as SQL injection and cross-site scripting, especially in custom web applications.
   xii. Other Applications: Scan for vulnerabilities in various applications like streaming media or proxy servers.
   xiii. Common Services: Identify vulnerabilities in services like file sharing and email.
   xiv. Wireless Access Points: Detect vulnerabilities and misconfigurations in wireless networks.
   xv. Backdoors/Malware: Identify the presence of malicious software like rootkits and Trojans.
   xvi. SL/TLS: Detect insecure cryptographic protocols and configurations, ensuring compliance with strong cryptography standards.
   xvii. Anonymous Key-Agreement Protocols: Identify and report the use of insecure cryptographic protocols that lack server authentication.
   xviii. Remote Access: Detect insecure remote access software configurations that could compromise the environment.

3.3. Scanning Tasks

Internal vulnerability scans must be performed from a credentialed scanning perspective. External vulnerability scans can be performed from an uncredentialed scanning perspective.

3.4. Vulnerability Identification

A process must be established to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and use an appropriate scoring system for gaming security (e.g. CVSS, ISO/IEC 31010, etc.), to assign a risk ranking (for example, as "High Risk," "Medium Risk," or "Low Risk") to newly discovered security vulnerabilities. The scoring system used must be identified in the scanning results.

3.5. Scanning Results

The Gaming Enterprise must submit verification of scans to the regulatory body and include a remediation plan and any risk mitigation plans for those vulnerabilities not able to be resolved.

a. Re-scans must occur until all “Medium Risk” vulnerabilities are resolved and/or accepted via a formal risk acceptance program.
b. All verified vulnerabilities must be corrected by the Gaming Enterprise and documented in a report provided to the regulatory body and testing be repeated after corrections are made to verify the vulnerability has been addressed.

3.6. Scanning Qualifications

The quarterly scans must be performed by either an ISF, regulatory body staff, or via a qualified employee of the Gaming Enterprise who is separate, in organizational terms, from the function which implements changes to the GPE.

APPENDIX: GAMING TECHNICAL SECURITY (GTS) TESTS

A. GTS Testing Methodologies

GTS testing must consist of an evaluation of GPE security by means of an attack simulation by an ISF following known vulnerability assessment and penetration testing methodologies as prescribed by the Open Source Security Testing Methodology Manual (OSSTMM), the Open Web Application Security Project (OWASP), the Penetration Testing Execution Standard (PTES), the National Institute of Standards and Technology (NIST) Technical Guide to Information Security Testing and Assessment SP800-115, and other specifications as needed. These methodologies ensure that information gathered throughout the GTS testing will be of sufficient detail to accurately assess the areas of risk exposure and their potential impact on the GPE.

NOTE: It is expected that testing related to network, system, and server security be performed on the live GPE. To prevent any disruption to live services, testing related to application security may be performed in a non-production environment (e.g. development environment, testing environment, etc.) which closely mirrors the GPE's setup to ensure accurate results.

A.1. White Box Testing

White Box Testing is conducted with full knowledge of the GPE's internal architecture, including access to source code, network configurations, and detailed documentation. This approach allows for a thorough examination of the system's inner workings, enabling the identification of vulnerabilities that may not be apparent through external testing.

A.2. Grey Box Testing

Gray Box Testing combines elements of both White Box Testing and Black Box Testing. The ISF has partial knowledge of the GPE's internal structure, often reflecting the perspective of a user with elevated privileges but not full administrative access. This approach simulates a scenario where an attacker has some insider knowledge and aims to test security controls with a semi-privileged perspective.

A.3. Black Box Testing

Black Box Testing is performed without any prior knowledge of the GPE's internal architecture. The ISF approaches the system as an external attacker would, attempting to identify and exploit vulnerabilities without any insider information. This type of testing is crucial for simulating real-world attack scenarios.

B. Vulnerability Assessment

Vulnerability assessments is a critical process for identifying vulnerabilities using up-to-date vulnerability databases, which could be later exploited during penetration testing by making basic queries relating to services running on the systems from which is possible to access sensitive data. Given the limited testing windows, the ISF should have full visibility and the ability to bypass certain protection, including all Service Provider security-enhancing services (e.g. Content Delivery Networks, Deep Packet Inspection, Denial of Service protection, Web Application Firewalls, etc.) to allow for a more accurate and comprehensive assessment by removing obstacles that could otherwise mask vulnerabilities. Vulnerability assessments may be performed using automated vulnerability scanners.

B.1. Internal Vulnerability Assessment

The Internal Vulnerability Assessment's objective is to identify security weaknesses within the internal infrastructure of the GPE. This assessment aims to uncover vulnerabilities that could be exploited by internal threats, compromised accounts, or attackers who have gained access to the internal network through external breaches or lateral movement.

a. The targets of this assessment are the internal-facing systems, which include:
   i. Servers within the DMZ or LAN.
   ii. Workstations and other network devices connected to the GPE.
   iii. Applications and services handling sensitive data or critical operations.

b. The ISF must perform a series of activities designed to identify and map the internal network, enumerate systems, and uncover security weaknesses:
   i. Network Surveying: A full mapping of the internal network to detect live hosts, network architecture, and connected devices. This phase helps define the internal attack surface.
   ii. Port Scanning: Identification of open ports on internal systems, revealing potentially exposed services that attackers can exploit.
   iii. System Identification (Enumeration): Detecting operating systems, device types, and services running on the network. This includes identifying all critical infrastructure devices and systems in the internal environment.
   iv. Service Enumeration: Gathering detailed information on running services and applications to understand their versions, configurations, and associated vulnerabilities.
   v. Uncredentialed Scanning: These vulnerability scans simulate an attacker with no internal access or valid credentials. They are used to identify open ports, services, and basic vulnerabilities visible to anyone who gains network access.
   vi. Credentialed Scanning: These vulnerability scans use valid credentials to perform a more thorough inspection of internal systems. They are used to reveal deeper insights into patch levels, configuration weaknesses, missing security controls, and improper permissions, providing a more comprehensive analysis of potential attack vectors.
   vii. Finding Validation and False Positive Elimination: The ISF should attempt to validate findings from the vulnerability scans to ensure that the reported issues are accurate. This includes manual verification of vulnerability details to confirm their legitimacy and the removal of false positives from the results, ensuring that only real, actionable risks are reported.
c. To ensure thorough coverage, the assessment must evaluate different layers of the network and technology stack, including host-level, network-level, and application-level security:
   i. Port and Service Scanning: The ISF will scan all systems and workstations to identify open ports and running services that may provide entry points for attackers.
   ii. Layer 2 VLAN Testing: The ISF must assess the configuration of VLANs, ensuring they are properly segmented and secured. This includes testing for unintended subnets or devices sharing the same broadcast domain.
   iii. Layer 3 Network Testing: Evaluation of VLANs that connect to public zones or the Internet DMZ, ensuring that there is no improper exposure of internal systems to external threats.
   iv. Comprehensive Vulnerability Enumeration: The ISF must enumerate all internal computers and network devices to provide a detailed inventory of vulnerabilities present on the network. This includes both active systems and passive infrastructure components such as switches, routers, and firewalls.
d. The use of credentialed scanning provides deeper insight into internal configurations and security posture. A sampling approach of 20%-30% of the GPE's inventory may be utilized for the scans, focusing on high-risk systems or those handling sensitive data. Credentialed scanning assesses configurations such as:
   i. User Permissions: Ensuring that access controls are properly enforced and that there are no excessive privileges granted to non-administrative users.
   ii. Patch Management: Identifying systems that are missing critical security patches or updates.
   iii. Configuration Weaknesses: Revealing misconfigurations that may expose sensitive data or allow unauthorized access.

B.2. External Vulnerability Assessment

The External Vulnerability Assessment's objective is to identify security weaknesses within the external-facing infrastructure of the GPE. This assessment aims to uncover vulnerabilities that could be exploited by external threats, unauthorized users, or attackers targeting publicly accessible systems.

a. The targets of this assessment are the external-facing systems, which include:
   i. Servers and devices accessible through public IP addresses.
   ii. Applications and services exposed to the internet that handle or transmit sensitive data.
   iii. Public-facing firewalls and network devices that protect the GPE's internal environment.
b. The ISF must perform a series of activities designed to identify and map the external network, enumerate exposed systems, and uncover security weaknesses:
   i. Network Surveying: A full mapping of the external network to detect live hosts, network architecture, and connected devices. This phase helps define the external attack surface.

ii. Port Scanning: Identification of open ports on external systems, revealing potentially exposed services that attackers can exploit.
iii. System Identification (Enumeration): Detecting operating systems, device types, and services running on the external network. This includes identifying all critical infrastructure devices and systems exposed to the internet.
iv. Service Enumeration: Gathering detailed information on running services and applications to understand their versions, configurations, and associated vulnerabilities;
v. Uncredentialed Scanning: These vulnerability scans simulate an attacker with no internal access or valid credentials. They are used to identify open ports, services, and basic vulnerabilities visible to anyone who gains network access.
vi. Finding Validation and False Positive Elimination: The ISF should attempt to validate findings from the vulnerability scans to ensure that the reported issues are accurate. This includes manual verification of vulnerability details to confirm their legitimacy and the removal of false positives from the results, ensuring that only real, actionable risks are reported.

c. Given the limited testing windows, the ISF should have full visibility and the ability to bypass certain protection, including all Service Provider security-enhancing services (e.g. Content Delivery Networks, Deep Packet Inspection, Denial of Service protection, Web Application Firewalls, etc.) to allow for a more accurate and comprehensive assessment by removing obstacles that could otherwise mask vulnerabilities. This ensures that the GPE's security posture is accurately evaluated, and no critical vulnerabilities are overlooked.

B.3. Application Vulnerability Assessment

The Application Vulnerability Assessment's objective is to identify security weaknesses across web, mobile, and desktop applications associated with the GPE. This assessment uses primarily automated scanning methods, complemented by manual validation to ensure accuracy. Potential security weaknesses may include flaws in input validation, authentication, session management, and other common areas of concern.

a. The targets of this assessment are the applications exposed to external users (B2C) and internal administrative portals (B2B) as part of the GPE, which include:
i. Public-facing applications accessible by patrons and external users.
ii. Web services, APIs, and other integral components of the GPE's operations.
iii. Business-to-business (B2B) integrations such as data feeds for odds, match data, and results; these services must be secure to prevent unauthorized access and data breaches.
iv. Back-office management portals used by partners, affiliates, or operators.

b. The ISF must perform a series of activities designed to identify and map the structure, including all accessible URLs and input points, and uncover security weaknesses.

c. The ISF must use industry-standard automated tools to scan the applications for vulnerabilities. These tools are designed to detect a wide range of common security issues, including injection vulnerabilities (e.g. SQL injection, Cross-Site Scripting, Command injection), authentication and session management flaws, security misconfigurations and out-of-date applications components and libraries:

d. After the automated scan, the ISF must manually validate the findings to ensure accuracy and remove false positives. This step confirms that only genuine vulnerabilities are reported, providing a reliable overview of the application's security posture

C. Penetration Testing

Penetration testing is a critical process for evaluating the security of the GPE by simulating an attacker's perspective by identifying and exploiting vulnerabilities that could compromise the confidentiality, integrity, and availability of the GPE. Penetration testing enables the ISF to validate the vulnerabilities identified during vulnerability scans and to assess the effectiveness of existing security controls under real-world attack scenarios.

C.1. Internal Network Layer Penetration Test

The Internal Network Layer Penetration Test's objective is to objective is to exploit identified vulnerabilities within the internal infrastructure of the GPE. This assessment simulates an attacker who has already gained a foothold within the internal network. The goal of this test is to uncover vulnerabilities that could be exploited by internal threats, compromised accounts, or attackers who have breached the external perimeter.

a. The targets of this test are the internal-facing systems, which include:
    i. Servers within the DMZ or LAN.
    ii. Workstations and other network devices connected to the GPE.
    iii. Applications and services handling sensitive data or critical operations.
b. During the test, the ISF must perform the following key activities:
    i. Reconnaissance and Information Gathering:
        1. Network Surveying: Mapping the internal network to identify live hosts, network architecture, and connected devices, defining the internal attack surface.
        2. System Identification (Enumeration): Identifying operating systems, device types, and services running on the network, focusing on critical infrastructure components.
    ii. Internal Network Scanning:
        1. Port Scanning: Identifying open ports on internal systems to detect potential entry points.
        2. Service Enumeration: Gathering detailed information on running services to assess their configurations and associated vulnerabilities.
    iii. Vulnerability Identification:
        1. Internal Vulnerability Scanning: Matching identified systems and services against known vulnerabilities to highlight missing patches, misconfigurations, and software flaws.
        2. Configuration and Access Control Review: Assessing user permissions, access controls, and system configurations to identify potential security gaps.
    iv. Attack Simulation:
        1. Initial Exploitation Attempts: Attempting to exploit identified vulnerabilities to gain unauthorized access within the internal network.
        2. Privilege Escalation and Lateral Movement: Testing for opportunities to escalate privileges and move laterally within the network to access additional systems and data.
    v. Segmentation and Isolation Testing:
        1. VLAN Effectiveness: Assessing how well VLANs and segmentation prevent breaches and limit lateral movement.
        2. Isolation Measures: Evaluating isolation techniques to ensure they effectively contain threats and restrict unauthorized access.
    vi. Access Control Validation:
        1. Lateral Movement Restriction: Ensuring access controls are configured to prevent unauthorized lateral movement within the network.
        2. Critical System Protection: Verifying that access controls effectively block unauthorized access to key systems

C.2. External Network Layer Penetration Test

The External Network Layer Penetration Test's objective is to exploit identified vulnerabilities within the external-facing infrastructure of the GPE. This assessment simulates an attack by an external threat actor attempting to breach the GPE through its external-facing systems. The goal of this test is to uncover vulnerabilities that could be exploited by external attackers to gain unauthorized access, disrupt operations, or exfiltrate sensitive data.

a. The targets of this test are the external-facing systems, which include:
    i. Servers and devices accessible through public IP addresses.
    ii. Applications and services exposed to the internet that handle or transmit sensitive data.
    iii. Public-facing firewalls and network devices that protect the GPE's internal environment.
b. During the test, the ISF must perform the following key activities:
    i. Reconnaissance and Information Gathering:
        1. Domain-based Discovery: Identification of publicly available information related to the GPE, including domain names, IP addresses, and associated services.
        2. Network Profiling: Mapping the external attack surface, including identifying the network topology, active services, and potential entry points.
    ii. External Network Scanning:
        1. Port Scanning: Identifying open ports on external-facing systems to detect potential entry points.
        2. Service Enumeration: Gathering detailed information on exposed services, such as software versions and configurations, to assess potential vulnerabilities.

iii. Vulnerability Identification:
1. Vulnerability Scanning: Comparing discovered systems and services against up-to-date vulnerability databases to identify exploitable weaknesses.
2. Configuration and Patch Review: Assessing system configurations for security weaknesses, such as outdated software, weak configurations, or exposed services.

iv. Attack Simulation:
1. Initial Exploitation Attempts: Attempting to exploit identified vulnerabilities to gain unauthorized access to external-facing systems.
2. Privilege Escalation: If initial access is gained, attempting to escalate privileges to obtain higher levels of access.
3. Lateral Movement Testing: Testing for lateral movement opportunities that could allow an attacker to move deeper into the network from the compromised external system.

v. Bypass Testing:
1. Perimeter Defense Evaluation: Testing the effectiveness of perimeter defenses, including Web Application Firewalls (WAF), by attempting to bypass them.
2. Simulated Sophisticated Attacks: Simulating advanced attack techniques to evaluate how well security measures hold up against sophisticated threats.

C.3. Application Layer Penetration Test

The Application Layer Penetration Test's objective is to exploit identified vulnerabilities across all types of applications associated with the GPE, including web applications, mobile applications, and desktop applications. This test simulates real-world attack scenarios to assess the application's resilience against unauthorized access, data breaches, and other malicious activities. The test involves a structured approach, which includes automated scanning as a preliminary step followed by in-depth manual testing of core security areas to explore and validate security vulnerabilities. The testing will follow the applicable OWASP Security Testing Guides and will assess the applications for the OWASP Top 10.

a. The targets of this test are the applications exposed to external users (B2C) and internal administrative portals (B2B) as part of the GPE, which include:
i. Public-facing applications accessible by patrons and external users.
ii. Web services, APIs, and other integral components of the GPE's operations.
iii. Business-to-business (B2B) integrations such as data feeds for odds, match data, and results; these services must be secure to prevent unauthorized access and data breaches.
iv. Back-office management portals used by partners, affiliates, or operators.

b. During the test, the ISF must perform the following key activities:
i. Reconnaissance and Information Gathering:
1. Application Profiling: Gather detailed information about the application's architecture, including programming languages, frameworks, database technologies, backend communication protocols, third-party libraries, and security controls.
2. Reverse Engineering: Decompile the application to examine the source code, APIs, and third-party components for hardcoded secrets, sensitive data exposure, or insecure configurations.

ii. Authentication Testing:
1. Credential Policy Enforcement: Review the application's credential policy and ensure it enforces complexity requirements (length, characters, and periodic rotation).
2. Credential Storage Security: Assess the security of credential storage mechanisms, ensuring they are properly hashed and salted.
3. Multi-Factor Authentication (MFA) Evaluation: Evaluate the security, effectiveness, and proper implementation of MFA and test for potential bypass techniques.
4. Brute-Force Attack Resilience: Test resilience against brute-force attacks, including account lockout and CAPTCHA implementations.
5. Token-Based Authentication: Test the security of authentication tokens (JWTs, OAuth tokens) used by the application to interact with backend services.

iii. Authorization Validation:
1. Role-Based Access Control (RBAC) Testing: Test for role enforcement across the application, ensuring that users with different permission levels can only access authorized areas, functions, and data appropriate for their roles.

2. Privilege Escalation Testing: Test for privilege escalation vulnerabilities, including both horizontal and vertical escalation by exploiting API endpoints, application functionality, or insecure backend configurations.
3. Authorization Bypass Testing: Attempt to bypass authorization controls through URL manipulation, parameter tampering, or direct object references. Attempt to access unauthorized areas using different privilege levels.

iv. Session Management Testing:
1. Session Handling Review: Collect and analyze session cookies, headers, and server-side tokens for potential misuse or misconfigurations.
2. Session Token Security Verification: Verify session token security, including randomness, uniqueness, and protection against exposure via URL parameters or insecure cookies. Ensure tokens expire correctly, are not reused, and are properly handled on logout.
3. Session Expiration and Timeout Assessment: Assess session expiration and timeout mechanisms to ensure sessions are appropriately terminated after inactivity or logout.
4. Session Hijacking Vulnerability Testing: Test for session hijacking vulnerabilities, such as capturing session cookies or exploiting session fixation vulnerabilities.
5. Secure Cookie Attribute Implementation: Ensure secure cookie attributes are in place, such as HttpOnly and Secure flags.

v. Input Validation and Injection Attacks:
1. Input Validation Review: Ensure that user input fields (such as username, password, search fields, etc.) are properly validated to prevent common application vulnerabilities.
2. Injection Attacks: Test the application for vulnerabilities that could allow an attacker to inject malicious code, SQL, command, script, and LDAP injection (e.g. JavaScript or malicious payloads), within the application and its interactions with backend services.
3. File Upload Handling Assessment: Assess file upload handling to ensure only permitted file types are accepted and processed securely, and that file size and content are validated. Ensure that file uploads restrict file types and validate inputs, preventing remote code execution.
4. Client-Side Validation Testing: Bypass client-side validation mechanisms and assess whether proper validation is being enforced server-side.

vi. Error Handling and Information Disclosure:
1. Error Message Sensitivity Assessment: Assess whether error messages reveal sensitive data about the application's internal workings that could aid an attacker in planning further attacks (e.g., stack traces, SQL errors).
2. Information Leakage Identification: Identify instances where sensitive data is inadvertently exposed through HTTP headers, error messages, or other communication channels.
3. Unexpected Error Handling Testing: Test how the application handles unexpected errors and whether sensitive data or system details are exposed during these failures.

vii. Integration and API Security:
1. API Evaluation: Evaluate the security of web services and APIs used in the GPE, ensuring they properly authenticate users, validate input, and prevent unauthorized access.
2. Token-Based Authentication Testing: Test the security of OAuth tokens or other API authentication mechanisms, ensuring proper handling and revocation processes.
3. Rate Limiting Assessment: Assess the implementation of rate-limiting mechanisms to prevent denial-of-service (DoS) attacks and abuse.

viii. Secure Configuration and Hardening:
1. Secure Communication Assessment: Verify the use of HTTPS with modern encryption standards (TLS 1.2 or higher) across all communication channels between the client and the server.
2. Data-in-Transit Security Testing: Test whether data transmitted between the application and backend services is encrypted using strong encryption (TLS 1.2+).
3. Man-in-the-Middle (MITM) Attacks: Test the application's vulnerability to MITM attacks, ensuring that traffic cannot be intercepted or modified by an attacker. Ensure that certificates are validated.
4. Minimal Service Exposure Review: Confirm that no unnecessary services or open ports are running on the server that could increase the attack surface.
5. Certificate Pinning Evaluation: Verify that the application implements certificate pinning to prevent the use of forged certificates during communication with the backend server.

ix. Local Data Storage Testing:
    1. Insecure Data Storage Testing: Test for sensitive data stored insecurely on the device, including hardcoded credentials, personal data, tokens, and session cookies stored in plaintext or weakly encrypted formats.
    2. File and Directory Permissions Verification: Verify that file permissions are correctly set, ensuring that only authorized users can access critical files.

x. Patch Management and Update Testing:
    1. Secure Update Mechanism: Ensure that updates are delivered securely and verify the integrity of the update packages.
    2. Patch Application: Test whether critical patches are applied promptly to the application and its dependencies.

xi. Application Logic and Workflow Testing:
    1. Transaction Processing Flaw Testing: Test for flaws in transaction processing, such as underpayments, overpayments, or manipulation of transaction amounts.
    2. Workflow Manipulation Assessment: Assess whether workflows can be bypassed or manipulated, allowing users to perform unauthorized actions or skip critical steps.
    3. Functionality Abuse Testing: Test for abuse of functionality scenarios where legitimate functions can be misused for unintended actions, such as reusing promo codes or exploiting refund mechanisms.
    4. Wagering and Payout Accuracy Validation: Validate that the application processes wagers accurately and securely reflect patron balances, winnings, and transaction history.
    5. Event Wagering API Security: Ensure APIs delivering match data, results, or odds are secure and cannot be tampered with.
    6. Patron Balance Security Testing: Test the accuracy and security of patron balances, ensuring that deposits, withdrawals, wagers, and winnings are correctly reflected.
    7. Bonus and Promotional Offer Validation: Validate the implementation of bonus and promotional offers, ensuring they cannot be abused, bypassed, or manipulated through logic flaws.
    8. Transaction Replay Prevention: Ensure that transaction replays or retries (such as placing a bet again) cannot lead to duplicate transactions or unauthorized gains.
    9. Multiple Account Detection Assessment: Assess the application's ability to detect and prevent the use of multiple accounts to manipulate odds, exploit bonuses, or engage in collusion.

xii. Third-Party Components and Libraries:
    1. Third-Party Library Security: Review and assess the integrity and security of any third-party libraries and dependencies used by the application used by the app, ensuring they are up to date and free from known vulnerabilities.
    2. Insecure API Use: Test for improper use of APIs, such as insecure implementations of biometric authentication, camera, microphone, and other device features.
    3. Dependency Management: Analyze the third-party libraries used within the application, checking for any outdated or vulnerable components that could compromise the security of the application.

c. For testing applications which are which are run from a server (web applications), the ISF must perform the following additional testing activities:

i. Public Information Collecting:
    1. Passive Information Collecting: Collect information about the application using non-intrusive methods, such as Google dorking, to discover publicly accessible data.
    2. Technology Profiling: Perform WHOIS lookups, DNS enumeration, and technology fingerprinting to gather details about the application's infrastructure and services.

ii. Cross-Site Handling:
    1. Cross-Site Scripting (XSS) Testing: Test input fields and URL parameters for XSS and other input-related attacks, ensuring inputs are properly sanitized and encoded. Verify that data presented to users is properly sanitized and encoded to mitigate XSS and other output-related attacks.
    2. Cross-Site Request Forgery (CSRF) Evaluation: Evaluate the application's resilience against CSRF attacks, ensuring proper use of anti-CSRF tokens to protect against unauthorized requests.

iii. Security Header Usage:
1. Security Header Implementation: Ensure the correct implementation of essential security headers like Content Security Policy (CSP) and Strict-Transport-Security (HSTS) to protect against common web vulnerabilities.
2. Security Header Configuration: Verify that additional security headers, such as X-Content-Type-Options, are properly configured to prevent MIME type sniffing and other attacks.

a. For testing applications which are installed to a user's device (mobile applications and desktop applications), the ISF must perform the following additional testing activities:

i. Tamper Resistance:
1. Binary Security: Examine the application binaries for weaknesses, ensuring that sensitive data (e.g., user credentials) is not stored in insecure formats or embedded in the application.
2. Obfuscation Techniques: Verify that the application code is obfuscated to prevent reverse engineering and code tampering by malicious actors.
3. Anti-Tampering Mechanisms: Test for the presence of anti-tampering mechanisms that prevent or detect unauthorized changes to the application binaries or configuration files.
4. Application Self-Protection: Check whether the application can detect tampering or the presence of debuggers and prevent malicious actors from modifying the application in real-time.
5. Rollback Protection: Ensure that the application prevents attackers from rolling back to a vulnerable version.

ii. Sensitive Data and Communication Security:
1. Data Caching and Temporary Files: Ensure that sensitive data is not cached insecurely or left in temporary files after the application is closed.
2. Clipboard Usage: Verify that sensitive data is not unintentionally stored or accessible via the clipboard (e.g., copying passwords or credit card information).
3. Inter-Process Communication (IPC) Attacks: Check for vulnerabilities in how the application communicates with other processes, ensuring that no unauthorized data can be injected.

iii. Memory Safeguards:
1. Buffer Overflow Vulnerabilities: Test for buffer overflow vulnerabilities that could lead to remote code execution.
2. Memory Corruption: Ensure that memory protections, such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR), are in place.

iv. Virtualization and Debugging Protections:
1. Virtual Machine Detection: Ensure that the application can detect and prevent being run in a virtualized environment, which could be used to manipulate or reverse-engineer the software.
2. Anti-Debugging: Test for the presence of anti-debugging techniques that prevent the use of debugging tools to reverse-engineer the application.

v. Additional Mobile Application Testing Tasks:
1. App Store Metadata Analysis: Identify the application's platform (iOS/Android) and review the app store listing, version history, developer information, and permissions requested by the app during installation.
2. Keychain/Keystore Security: Test whether sensitive data is stored securely using the Android Keystore or iOS Keychain, ensuring that proper cryptographic standards are followed.
3. Jailbreaking/Root Detection: Verify that the application can detect and respond to execution in a jailbroken (iOS) or rooted (Android) environment, limiting access to critical features.

D. Cloud and Container Security Assessment

The Cloud and Container Security Assessment ensures the secure deployment, management, and operation of cloud and containerized environments within the Gaming Production Environment (GPE). This assessment focuses on the security of cloud-based components, containerized applications, and the supporting orchestration frameworks to minimize risks and improve security resilience.

D.1. Cloud Security Assessment

The Cloud Security Assessment's objective is to ensure the secure management of cloud-based components within the GPE, ensuring that cloud-specific security controls and configurations are properly implemented and managed. This assessment covers the following:

a. Access Controls: Verify that access policies enforce the principle of least privilege, and that strong authentication methods, such as multi-factor authentication, are implemented for critical accounts.
b. Account Management: Assess the processes for account creation, management, and deactivation. Ensure roles and permissions are appropriately defined and inactive or unnecessary accounts are promptly removed.
c. Logging and Monitoring: Confirm that all critical actions, such as access to sensitive data and configuration changes, are logged and securely stored. Ensure that monitoring and alerting mechanisms are in place to detect and respond to potential security incidents.
d. Security Configuration: Review network and resource configurations to ensure proper segmentation, isolation, and traffic control. Verify that sensitive data is encrypted and that encryption keys are securely managed.
e. Firewall Rule and Policy Review: Ensure that cloud-specific firewalls (e.g., security groups, cloud-native firewall policies) are correctly configured to restrict access based on least privilege.
f. Service and Application Isolation: Review the segmentation of cloud services and applications, ensuring they are properly isolated from each other to minimize the risk of lateral movement by attackers.

D.2. Container Security Assessment

The Container Security Assessment's objective is to evaluate the security posture of GPEs utilizing container-based technology (e.g., Kubernetes) by identifying vulnerabilities, misconfigurations, and potential threats to ensure the integrity, confidentiality, and availability of applications and data. This assessment covers the following:

a. Container Configuration:
    i. Secure Image Management: Ensure container images are from trusted sources, regularly scanned for vulnerabilities, and minimized to reduce attack surfaces.
    ii. Configuration Hardening: Verify containers are configured according to best practices, with unnecessary services disabled and resource limits enforced.
b. Orchestration Security:
    i. Cluster Security: Assess the security of the orchestration platform, including control plane configurations, node security, and workload isolation.
    ii. Access Control: Review RBAC settings to ensure proper permission assignments and restricted administrative access.
    iii. Network Policies: Evaluate network segmentation and traffic control within the container environment to ensure secure and restricted communication.
c. Runtime Security:
    i. Monitoring and Threat Detection: Implement and review monitoring of container runtime behavior to detect anomalies and respond to threats.
    ii. Patch Management: Ensure that container images are updated with the latest security patches and that outdated images are not deployed.
d. Supply Chain Security:
    i. Dependency Management: Monitor and manage third-party libraries and dependencies to reduce the risk of supply chain attacks.
    ii. Pipeline Security: Secure the CI/CD pipeline to ensure only verified and secure code is deployed.

E. Additional Assessments and Tests

E.1. Firewall Security Assessment

The Firewall Security Assessment's objective is to identify potential weaknesses in the firewall configurations, rule sets, and management practices. This assessment ensures that the firewall is appropriately configured and managed to effectively prevent unauthorized access and mitigate security threats, in line with the organization's security policies and industry best practices. This assessment covers the following:

a. Network Architecture Analysis:
    i. Understanding the Environment: The ISF must begin by thoroughly understanding the GPE's network architecture, including the assets the firewall is meant to protect and the potential threats to those assets.
    ii. Design Flaw Identification: The assessment starts with evaluating the placement of the firewall within the network to identify any design flaws or vulnerabilities in its current deployment compared to industry best practices.
b. Rule Set Review:
    i. Least Privilege Rule Configuration: Ensure rules are configured according to the principle of least privilege.
    ii. Connection Restriction Confirmation: Confirm that inbound and outbound connections are restricted to necessary services only.
    iii. Network Address Translation (NAT) Verification: Verify that NAT is properly implemented.
    iv. Protocol Blocking Assessment: Ensure all unknown or undefined protocols are blocked.
    v. Cleanup Rule Presence Confirmation: Confirm the presence of a "clean-up" rule to handle unspecified traffic.
    vi. Rule Documentation Review: Review and confirm that rules are appropriately documented and temporary rules are disabled or removed when no longer needed.
c. Configuration Settings Review:
    i. Unauthorized Access Configuration Identification: Identify any configuration settings that could allow unauthorized access or compromise the security of the systems protected by the firewall.
    ii. Firewall Policy Compliance Verification: Verify that the firewall configuration aligns with the organization's security policies and industry best practices.
d. Central Management Console Review:
    i. Access Control: Ensure that only authorized personnel can access the firewall management console, and that access controls are properly enforced.
    ii. Console Protection: Confirm that the management console is adequately protected against unauthorized access, including the use of encrypted protocols for remote management.
e. Logging, Auditing, and Monitoring:
    i. Logging Configuration: Ensure that logging is enabled for security events (e.g., failed logins) and that logs are configured to capture relevant data.
    ii. Log Management: Confirm that logs are written to a central location, backed up regularly, and reviewed periodically for suspicious activity.
    iii. Monitoring and Alerting: Verify that alerting mechanisms are in place to provide real-time visibility into potential security incidents.
f. Patch Management:
    i. Patch Implementation: Confirm that a system exists for testing patches before deploying them on production firewalls, and that all security-related patches are applied promptly.
    ii. Patch Review: Assess whether the firewall's firmware and software are up to date and in line with security best practices.
g. Remote Access Security:
    i. Protocol Security: Ensure that unnecessary protocols for accessing the firewall are disabled and that remote access is only allowed over secure, encrypted protocols.
    ii. Access Restrictions: Verify that remote access to the firewall is restricted to trusted networks and specific IP addresses.
    iii. Traffic Filtering: Confirm that traffic filtering is appropriately set up to control data flow between cloud environments and between cloud and on-premises infrastructures.
h. Virtual Network Security:
    i. Network Segmentation: Assess the segmentation within virtual networks, ensuring that sensitive data and critical services are isolated from less secure areas.
    ii. Cross-Environment Traffic Management: Ensure secure management of traffic between different cloud environments, as well as between cloud and on-premises systems, with a focus on encryption and integrity protection.
i. Identity and Access Management (IAM) Integration:
    i. Access Control Policies: Ensure that IAM policies are integrated with cloud firewalls to enforce strict access control and role-based access.

ii. Multi-Factor Authentication (MFA): Verify that MFA is enforced for accessing cloud firewall configurations and management consoles.

j. Automation and Orchestration:
   i. Configuration Automation: Assess the use of automation tools to manage and enforce firewall rules and configurations across cloud environments, ensuring consistency and reducing human error.
   ii. Policy Compliance: Confirm that automated compliance checks are in place to ensure firewall configurations remain aligned with security policies and best practices.

E.2. Database Security Assessment

The Database Security Assessment's objective is to ensure that databases, which store sensitive data such as PII, financial transaction data, and gaming-related data, are secure from unauthorized access and are compliant with best practices and applicable regulatory standards. This includes reviewing the encryption mechanisms and the general security of the database environment, including data-at-rest and data-in-transit protections. This assessment follows the OWASP guidelines for Cryptographic Storage and other industry standards, ensuring the security and confidentiality of the GPE's sensitive data. This assessment covers the following:

a. Documentation Review: Process documentation is requested from the client and analyzed for completeness and alignment with best practices.
   i. Configuration Review:
      1. Secure Configuration Baseline: Verify the overall configuration of the database environment to ensure that services, ports, and user accounts are configured securely. Look for any unnecessary services that could increase the attack surface.
      2. Backup and Recovery Procedures: Review how backups are managed and ensure they are encrypted and stored securely. Backup and recovery procedures must include encryption during transit and storage.
      3. Audit and Logging Settings: Verify that auditing is enabled for critical actions such as access to sensitive data, configuration changes, and privilege escalation attempts. Ensure logs are securely stored and regularly reviewed.
      4. Data Encryption Methods: Assess whether data-at-rest and data-in-transit encryption is applied properly, using industry-standard encryption algorithms (e.g., AES-256).
   ii. Access Control and Authentication:
      1. Role-Based Access Control (RBAC): Review access control policies to ensure only authorized users have access to sensitive databases. Confirm that user roles are assigned based on the principle of least privilege.
      2. Multi-Factor Authentication (MFA): Ensure that critical database accounts, such as administrators, are protected with multi-factor authentication.
      3. User Account Management: Assess the processes for creating, managing, and deactivating database user accounts, ensuring that inactive or unnecessary accounts are removed or disabled.
   iii. Vulnerability Scanning and Patching:
      1. Regular Vulnerability Scans: Ensure that vulnerability scans are performed regularly to detect and address database software vulnerabilities, outdated patches, and misconfigurations.
      2. Patch Management: Verify that critical patches are applied promptly and that outdated database versions are retired or properly secured.
      3. Database Hardening: Review the security hardening measures taken to prevent common database vulnerabilities, such as SQL injection attacks and misconfigurations.
   iv. Data Protection and Privacy Controls:
      1. Data Masking and Tokenization: Ensure that data masking is applied to non-production environments, especially for databases containing sensitive data.
      2. Database Activity Monitoring (DAM): Ensure that database activity monitoring tools are in place to detect anomalous behavior or unauthorized access attempts.
      3. Encryption Key Management:
      4. Key Storage and Access Controls: Ensure encryption keys are securely stored and protected using a Trusted Platform Module (TPM) or Hardware Security Module (HSM), and that access is tightly controlled and logged.

5. Key Rotation and Expiration: Review policies and procedures for key rotation, expiration, and revocation, ensuring that key lifecycles are managed securely.

v. Network Security and Isolation:
   1. Database Segmentation: Ensure that databases are properly segmented from less secure network segments. Access should be restricted based on IP whitelisting and network zoning.
   2. Firewall Configuration: Confirm that firewalls are in place to prevent unauthorized access to the database servers and that secure protocols are used for communication between the database and application servers.
   3. Encrypted Communication: Verify that all communication between the database and clients or applications is encrypted using TLS/SSL.

b. Live Interview and Demonstration: A video interview is conducted with the Database Administrator (DBA), who demonstrates live configurations and queries on the database system, allowing verification of security controls in action.
   i. Configuration Verification: During the interview, visually verify configurations in the database to ensure encryption and security controls match the documentation.
   ii. Demonstration of Encryption: Request the DBA to demonstrate how encrypted data is stored and accessed, ensuring that sensitive data (e.g., patron accounts, PII) is encrypted properly and complies with regulatory requirements.
   iii. Password Storage Verification: Ensure the DBA runs queries that show how passwords are stored (hashed and salted) and verify that older records also follow proper encryption protocols.
   iv. Data Encryption and Access Controls: Review and confirm the encryption of PII such as legal names, government identification numbers (social security numbers, taxpayer identification numbers, passport numbers, or equivalent), and personal financial information (credit or debit instrument numbers, bank account numbers, etc.), ensuring that all sensitive fields are encrypted.

E.3. Social Engineering Security Assessment

The Social Engineering Security Assessment's objective is to test the human element of the GPE's security, identifying vulnerabilities that could be exploited through manipulation rather than technical means. This assessment helps identify weaknesses in human behavior and physical security that could lead to breaches, ensuring a more holistic approach to protecting the GPE. This assessment covers the following:

a. Human Behavior:
   i. Phishing Campaigns: Simulate targeted phishing attacks to assess the effectiveness of employee training and the GPE's ability to detect and report suspicious emails.
   ii. Vishing and Pretexting: Conduct phone-based social engineering attempts to extract sensitive data or gain unauthorized access by impersonating trusted entities.
   iii. Spear Phishing: Tailored phishing attacks directed at high-value targets within the organization to test the robustness of executive and privileged access account protections.

b. Physical Security:
   i. Physical Intrusion Attempts: Test the physical security measures by attempting to gain unauthorized access to restricted areas within the GPE, assessing the effectiveness of security protocols.
   ii. Device Compromise: Attempt to plant unauthorized devices within the facility to intercept communications or exfiltrate data, evaluating the physical security controls in place.
   iii. Access Badge Cloning: Test the resilience of physical access controls by attempting to clone employee access badges and gain entry to secure areas.

E.4. Wireless Security Assessment

The Wireless Security Assessment's objective is to evaluate the security and reliability of the wireless infrastructure within the GPE. This assessment focuses on identifying vulnerabilities, misconfigurations, and weaknesses in the wireless networks that could lead to unauthorized access, data interception, or other forms of exploitation. It ensures that the wireless networks supporting the GPE are secure, resilient, and properly managed according to security best practices. The assessment involves a structured approach, combining active and passive scanning, configuration reviews, and vulnerability testing. This assessment covers the following:

a. The targets of this test are the wireless access points (WAPs), wireless networks, and any associated wireless infrastructure within the GPE, which include:
   i. Public-facing networks used by patrons, visitors, or contractors.
   ii. Internal wireless networks used by employees for administrative or operational purposes.
   iii. Guest networks and segregated wireless access for non-critical use.
   iv. Wireless devices used for internal operations, such as handheld terminals, tablets, or other mobile devices connecting to the GPE's wireless infrastructure.

b. During the test, the ISF must perform the following key activities:
   i. Reconnaissance and Information Gathering:
      1. Wireless Access Point Mapping: Map all WAPs on the GPE network to identify all devices broadcasting or connecting to the wireless infrastructure.
      2. Network Surveying: Scan the wireless networks to identify Service Set Identifiers (SSIDs), devices connected to the network, and access points broadcasting within the environment.
      3. Rogue Access Point Detection: Identify unauthorized or rogue access points that may have been maliciously or mistakenly added to the network.
   ii. Configuration and Security Review:
      1. Encryption and Access Controls: Ensure that strong encryption protocols, such as WPA3 or WPA2 with AES, are in use across all wireless networks and that legacy encryption protocols (e.g., WEP) are disabled. Review access controls to ensure proper segmentation of guest, public, and internal networks.
      2. SSID Management: Assess whether SSIDs are being broadcast unnecessarily and ensure hidden SSIDs are configured for critical networks.
      3. Authentication and Authorization: Ensure that authentication mechanisms (e.g., 802.1x) are correctly implemented and enforced, preventing unauthorized devices or users from accessing sensitive networks. Verify the correct use of captive portals and pre-shared keys, where applicable.
      4. Network Segmentation: Review segmentation between public, guest, and internal networks to ensure that access to critical systems is restricted and monitored.
      5. Vulnerability Identification: Identify vulnerabilities against up-to-date vulnerabilities databases, including any unpatched firmware on wireless devices.
   iii. Intrusion Detection and Monitoring:
      1. Rogue Access Point Detection: Ensure systems are in place to detect and alert administrators to unauthorized wireless devices or rogue access points. Implement continuous monitoring to detect any unusual activity on the wireless networks.
      2. Wireless Intrusion Detection System/Intrusion Prevention System (IDS/IPS): Assess the effectiveness of any Wireless IDS or IPS in identifying and preventing attacks such as deauthentication, jamming, or man-in-the-middle (MITM) attacks.
   iv. Active and Passive Wireless Testing:
      1. Passive Testing: For high-traffic wireless environments, passive scanning methods are utilized to monitor and analyze wireless traffic without interacting with the network.
      2. Active Testing: In low-traffic or secure areas, active testing methods (e.g., attempting to connect, vulnerability exploitation, or handshake capture) must be performed to assess the resilience of the wireless infrastructure.
      3. Bleed Testing: Assess the wireless signal range to ensure it does not bleed outside the intended coverage area, which could expose the network to attackers.
   v. Wireless Network Performance and Signal Coverage:
      1. Signal Coverage Mapping: Assess the placement and signal strength of wireless access points to ensure that the wireless signal does not extend beyond the secure perimeter. Ensure consistent and reliable coverage within intended areas, such as key operational zones within the GPE.
      2. Performance Evaluation: Test the ability of the wireless network to handle peak traffic loads without degradation in performance or security.
   vi. Firmware Updates: Ensure that all wireless access points and related infrastructure are running up-to-date firmware to protect against known vulnerabilities.
   vii. Wireless Network Policies:
      1. Ensure the wireless network complies with organizational security policies, gaming industry standards, and relevant regulations (e.g., PCI DSS, GDPR, etc.).

2. Confirm that guest and public networks follow a separate set of policies to avoid any overlap or unauthorized access to critical internal networks.

viii. Logging and Auditing: Verify that logging mechanisms are enabled on all access points and that access logs are securely stored and regularly reviewed for signs of unauthorized activity.

ix. Physical Security: Confirm that wireless network devices (e.g., access points and controllers) are secured physically, with access restricted to authorized personnel only.

E.5. Source Code Security Assessment

The Source Code Security Assessment's objective is to detect security vulnerabilities, including both common issues and more complex threats specific to the GPE, through both manual review and the use of automated tools. This assessment covers the following:

a. Automated Code Scanning: Automated tools are used to scan the source code for known vulnerabilities and code patterns that may indicate security flaws.

b. Manual Code Review: In-depth manual inspection is performed on critical areas such as transaction handling, game logic, and authentication systems.

c. Authentication and Authorization: Ensure secure mechanisms for user authentication and access control. Verify the robustness of multi-factor authentication (MFA) and session management systems to prevent unauthorized access.

d. Input Validation and Output Encoding: Validate all user inputs to ensure they are properly sanitized to avoid common vulnerabilities like SQL Injection and Cross-Site Scripting (XSS). Ensure that output data is securely encoded before being returned to users.

e. Sensitive Data Handling: Assess how sensitive data such as PII (Personally Identifiable Information) and payment information are handled, ensuring encryption for data both in transit and at rest. Evaluate the management of encryption keys to prevent exposure.

f. Error Handling and Logging: Review error handling procedures to ensure that sensitive system information is not disclosed through error messages. Logs must be appropriately secured and avoid logging sensitive data such as user credentials.

g. Game Logic Security: Analyze the implementation of core game logic, including Random Number Generator (RNG) mechanisms, to ensure fairness and integrity. Secure RNG implementations are crucial for preventing manipulation of game outcomes.

h. Third-Party Libraries and Dependencies: Ensure that all external libraries used in the application are up to date and free from known vulnerabilities. Regularly audit dependencies as part of the secure development lifecycle.

E.6. Adversarial Simulation Test

The Adversarial Simulation Test's objective is to enhance the security posture of the GPE by simulating sophisticated, real-world attack scenarios across the entire spectrum of potential attack vectors, focusing on both digital and physical aspects of security. This test is designed to stress-test the GPE's resilience against a range of advanced tactics, techniques, and procedures used by real-world attackers. The goal is to evaluate the GPE's ability to detect, respond to, and mitigate advanced attack techniques that determined threat actors might employ. This test covers the following:

a. Unlike traditional penetration tests, this test mimics a highly skilled, persistent adversary aiming to breach the GPE's defenses using any means necessary.

b. During the test, the ISF must perform the following key activities:

i. Open Source Intelligence (OSINT) and Information Gathering:

1. Publicly Available Information: Collect and analyze publicly available information about the Gaming Enterprise, its infrastructure, employees, and partners.

2. Domain Registration and DNS Information: Gather data from WHOIS records, DNS lookups, and domain registration details to identify potential attack vectors related to domain management.

3. Social Media Profiling: Analyze social media accounts of key employees to gather information that could be leveraged in social engineering attacks.

4. Publicly Accessible Documentation: Search for publicly accessible documents, such as PDFs, presentations, and reports, that might contain employee names, email addresses, internal processes, or other sensitive data.
5. Data Breach and Leak Searches: Investigate whether any company-related data has been exposed in previous breaches, including credentials, email addresses, or other sensitive data.
6. Technical Footprinting: Identify external-facing infrastructure, services, and technologies used by the GPE through passive reconnaissance techniques such as banner grabbing, search engine queries (e.g., Google dorking), and public security databases.
7. Third-Party Relationships: Research partnerships, vendors, and third-party services used by the Gaming Enterprise to identify potential supply chain vulnerabilities.

ii. Advanced Network Attacks:
1. Lateral Movement: Simulate an internal attacker who has gained initial access, testing the ability to move laterally across the network to access sensitive systems.
2. Persistence Mechanisms: Test the GPE's defenses against attackers attempting to establish long-term persistence within the network, ensuring detection and removal of malicious footholds.
3. Data Exfiltration: Simulate the methods an attacker might use to exfiltrate sensitive data from the GPE, testing the effectiveness of data loss prevention (DLP) measures.
4. Advanced Reconnaissance: Perform stealthy network discovery and reconnaissance to map the internal network and identify key assets and systems for targeted attacks.
5. Command and Control (C2) Testing: Establish and maintain communication with compromised systems using various C2 techniques to test the organization's detection capabilities.
6. Privilege Escalation: Test the ability to escalate privileges from lower-level access to administrative or root access, leveraging system misconfigurations or vulnerabilities.
7. Credential Dumping and Reuse: Attempt to extract and reuse credentials from compromised systems to further infiltrate the network or access sensitive data.

iii. Incident Response Evaluation:
1. Detection and Alerting: Assess the effectiveness of the GPE's monitoring and alerting systems in detecting sophisticated attack activities, ensuring timely response.
2. Response and Containment: Evaluate the speed and efficiency of the incident response team in containing and mitigating the simulated threats, focusing on minimizing impact.
3. Post-Incident Analysis: Review the GPE's ability to conduct thorough post-incident analysis, implement lessons learned, and enhance security defenses to prevent future incidents.

c. The results of the test will provide the Gaming Enterprise with a detailed understanding of how their security defenses perform against advanced attack scenarios. The findings will inform strategic security improvements and reinforce the importance of a proactive, layered defense strategy, ensuring the GPE remains robust against emerging threats.

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.
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.
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.
Backup	A copy of files and programs made to facilitate recovery if necessary.
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.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical Control Program	Software programs that control behaviors relative to any applicable technical standard and/or regulatory requirement, such as executables, libraries, gaming or system configurations, operating system files, components that control required system reporting, and database elements that affect gaming or system operations.
Critical System Component	Any hardware, software, critical control programs, communications technology, other equipment or components implemented in a GPE to allow patron participation in gaming, and whose failure or compromise can lead to loss of patron entitlements, government revenue or unauthorized access to data used for generating reports for the regulatory body. Examples of Critical System Components include, but are not limited to: • Components which record, store, process, share, transmit, or retrieve sensitive data. • Components that could impact the security of sensitive data or the GPE. • Components which generate, transmit, or process random numbers used to determine the outcome of games and events. • Components which store results or the current state of a patron's game, wager, or available funds.

Term	Descriptions
	• 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). • 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.
Denial of Service (DoS)	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 DoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.
Domain	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
Domain Name Service (DNS)	The globally distributed internet database which (amongst other things) maps machine names to IP numbers and vice-versa.
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.

Term	Descriptions
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.
Gateway	Any device, system, or software application that can perform the function of translating data from one format to another. The key feature of a gateway is that it converts the format of the data, not the data itself.
GIS Incident	An occurrence that actually or potentially jeopardizes the 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.
Hash Algorithm	A function that converts a data string into an alpha-numeric string output of fixed length.
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

Term	Descriptions
	computer and network activities and analyzing those events to look for signs of intrusion in the GPE.
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.
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 (MITM) 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.
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.
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.
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

Term	Descriptions
	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.
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: a. Audit logs and system databases recording information used to determine outcome, payment, redemption, and the tracking of patron information; b. Accounting and significant event information related to the Critical System Components of the GPE; c. RNG seeds and any other information which affects outcomes of games and wagers; d. Encryption keys, where the implementation chosen requires transmission of keys; e. Validation numbers associated with patron accounts, wagering instruments, and any other gaming transactions; f. Transfers of funds to and from patron accounts, electronic payment accounts, and for the purposes of gaming; g. Software packages within the GPE; h. Any location data related to employee or patron activity (e.g. account management, online gaming, etc.); i. 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 j. 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.

Term	Descriptions
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.
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).
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.
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.
Vulnerability	Software, hardware, or other weaknesses in a network or system that can provide a "door" to introducing a threat.
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.
Workstation	An interface for authorized personnel to access the regulated functions of the GPE.