

# iGaming Information Security Management: Is Your Business Adequately Protected?

A GLI WHITE PAPER



[GamingLabs.com](http://GamingLabs.com)



# Table of Contents

THE FIRST STEP – UNDERSTANDING YOUR SECURITY RISKS .....	3
INFORMATION SECURITY MANAGEMENT IN IGAMING.....	4
INFORMATION SECURITY FRAMEWORK OVERVIEW .....	5
CONFIDENTIALITY.....	5
INTEGRITY.....	6
AVAILABILITY.....	7
SECURITY ASSESSMENTS AND AUDITS.....	8
IMPLEMENTATION STEPS.....	10
ABOUT GLI.....	15

© Gaming Laboratories International, LLC 2016

The information contained in this white paper is for general guidance only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, the information in this document is provided "as is" without any warranty, express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement. GLI® assumes no liability resulting from errors or omissions in this document or from the use of the information contained herein.

Comments on the paper are welcome and should be addressed to Mrs. Christie Eickelman, VP of Marketing at +1 (702) 914 2220 or [c.eickelman@gaminglabs.com](mailto:c.eickelman@gaminglabs.com).



In one form or another, security measures have always been an integral part of gambling operations, whether simply to protect deposits and winning disbursements or to maintain the integrity of the gambling process.

Securing a land-based casino can be accomplished by controlling physical access to different parts of the casino and by restricting outside connections to the casino IT infrastructure. By design, this isn't possible in the case of Internet-based gambling (iGaming) systems, where constant exposure to the Internet through a public interface is needed to operate the business. The physical controls which operate to restrict access to the casino and manage patron activities must be replaced by logical controls and gateways. The face-to-face interactions used by casinos to verify patron information must be replaced by robust systems which provide the same level of assurance - but do so remotely. What hasn't changed from moving gambling to the Internet is that security is an integral part of business operations, and even though iGaming is built on the latest information technologies, security cannot just be a function of the IT department, but must be a commitment from the entire business.

## THE FIRST STEP – UNDERSTANDING YOUR SECURITY RISKS

Rather than adopting a piecemeal approach to the security of the information systems they control, Internet gaming operators should take the first step in establishing an information security management process – performing a risk assessment on your operations. This can be undertaken internally or by using outside consultants, such as GLI, to provide an assessment of your information security risks. Establishing a clear picture of the risks associated with your business should be part and parcel of the governance process.

Once the risks are understood, designing and setting up an information security framework is a well-established process: assess the vulnerabilities and threats to your information infrastructure, establish security objectives in line with an assessment of the risks posed by those threats and vulnerabilities, and implement the appropriate countermeasures to manage the risks.

The security objectives are commonly met by the implementation of known information security controls. The preferred approach uses layered security, which provides redundancy and reinforces the overall security model, as several layers of security must be breached before critical data stores can be accessed.

While no system can be absolutely secure against a determined, skilled and resourceful adversary, the implementation of these controls as part of an overall information security management system provides the most cost-effective defense against security breaches. However, these controls do not address the question of whether the implemented solutions actually work as intended. In order to provide validation that an information security system is working as intended, it must be fully audited and routinely monitored and tested thereafter.



# INFORMATION SECURITY MANAGEMENT IN iGAMING

Gaming is a highly regulated industry with regulators in each gaming jurisdiction establishing technical standards for the offering of fair, secure and auditable gaming operations within their jurisdiction. Early in the development of regulatory regimes for online gambling jurisdictions, it was realized that information security would be a significant factor that would need to be considered, and as a result, many iGaming technical standards have included security elements. These requirements extend to both the technical requirements of the gaming systems themselves and the internal controls needed to manage the gambling operations offered through the online gambling systems.

As the iGaming industry has matured, so have the security requirements of iGaming jurisdictions. The latest iterations of gambling technical standards and licensing requirements from many highly regulated jurisdictions have settled on the latest versions of ISO/IEC 27001:2013 as a general security standard and ISO/IEC 27002:2013 as implementation guidelines for information security management in iGaming jurisdictions. These are global standards and guidelines and provide a flexible baseline for information security management which can be applied to iGaming operations regardless of the variability in the individual businesses operators in this industry.

While these standards may be viewed as just another hoop to jump through, they should be seen, in fact, as an integral part of an evolving information security management strategy designed to ensure the security of the information held by the business. They are not prescriptive in the sense of defining at a detailed level what needs to be implemented, and a real understanding of the use of these ISO/IEC standards shows a way forward to integrate information security management within the overall business processes of the organization.

Some of the benefits of implementing the ISO 27001 standard are as follows:

- Brings your organization to compliance with legal, regulatory, and statutory requirements.
- Provides a process for Information Security and Corporate Governance.
- ISO 27001 certification is recognized on a worldwide basis and can be a market differentiator due to its recognition.
- Increase in overall organizational efficiency and operational performance.
- Minimizes internal and external risks to business continuity.
- Provides your organization with continuous protection that allows for a flexible, effective and defensible approach to security and privacy.

While it exists as a standard, ISO 27001 should be seen as part of the process of continually evolving improvement and adaptation to the needs of the iGaming business. The plan-do-check-act (PDCA) cycle of continuous refreshment and reinforcement associated with compliance enables a business to adapt their processes while still remaining compliant with the standard.

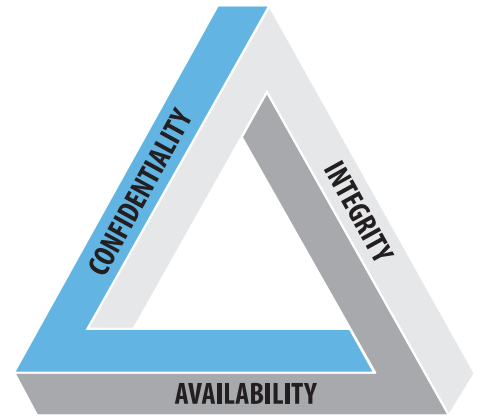
In addition, many of the security standards adopted by iGaming jurisdictions were based on the controls described in ISO 27001, as is the case for the UK, even if they were not as explicitly identified.

The key lesson in the adoption of a standard such as ISO/IEC 27001 is that this adherence to the standard reinforces for a business that information security is an integral part of business operations and requires the involvement of management at every level up to the C-suite.

## INFORMATION SECURITY FRAMEWORK OVERVIEW

Adherence to an information security management system standard, such as ISO/IEC 27001, does not necessarily make your information system secure. In addition to the controls and business processes that must be adopted as an inherent part of seeking compliance to a standard, such as ISO 27001, is the additional focus on the particular technical aspects of security, which can impact the iGaming business.

A commonly accepted information security framework uses the Confidentiality, Integrity and Availability triad, or CIA triad, as a model designed to guide policies for information security within an organization. The elements of the triad are considered the three most crucial components of information security and can be related back to operational requirements of the business.



How do these CIA triad components relate to iGaming security? This is summarized in the following sections, where we discuss how aspects of each of these areas can be related back to the security of online gambling operations.

### Confidentiality Keeping sensitive information secure

The first thought that comes to most people's minds when considering information security are the stories of security breaches which result in the loss of large amounts of personal information or expose people to possible identity theft or credit card fraud. This includes the highly publicized breaches of the Sony network and Las Vegas Sands Corporation and the hacks on Target and Home Depot.

Aside from the difficulties of being a part of cyberspace, Internet gaming systems have other risks associated with the nature of their business. The first is that Internet gambling sites collect a lot of personal information from their players. They don't do this in order to amass information, but in order to be able identify their players in a scenario where the player isn't across the desk from them, but may be located in a different country altogether. Unfortunately, the information that Internet gaming sites collect on their players to verify identity remotely is precisely the information needed for identity theft. There really isn't much difference between establishing your identity through the Internet for gambling purposes and establishing your identity as part of a scam.

Protecting all of this personal information is a prime consideration for Internet gambling sites because a release of personal information on a large scale could result in catastrophic losses for the business as well as legal issues if the Internet gambling site operates in a regime where breaches of personal information must be dealt with in a prescribed manner by law.

Web application vulnerabilities, which leave operators open to attacks, are well known - see, for example, the top 10 vulnerabilities list from the Open Web Application Security Project (OWASP). OWASP has also published guides to secure coding practices designed to protect web applications from the common attacks which exploit vulnerabilities resulting from insecure coding practices.

If approaches are already available and known to ensure the security of the web application interface from attack, then are there any other sources of vulnerabilities which should be considered in an iGaming context? There are two areas where the activities of online gambling operations may be exposed to confidentiality risks which are not directly related to the vulnerability of the web application software itself: gaps in security resulting from differences in the security posture of integrated architectures and gaps in security resulting from the access to the gaming platform granted to third-party service providers.

## Integrating Other Architectures

When a company that has a culture of stringent information security practices acquires another company with a different corporate culture and a different security philosophy, how far should they go to integrate the newly acquired products into their existing platform architecture? The best solution may be to leave the acquired product as an independent entity, but this is not always why the purchase was made. Then what are the security risks associated with the acquired product that will put your systems at risk?

**Industry consolidation through mergers and acquisition continues to increase. Securing each acquired asset or business unit on its own is no longer sufficient; an overall security strategy encompassing all business units must be in place to ensure there are no unintended gaps in security.**

One early consideration may be a data transfer between the information systems of the acquired company and those of the acquiring entity. In this case, not only must the data transfer be conducted in a secure manner to ensure the confidentiality of the data, but the integrity of the data must be maintained and a careful plan established to validate the data after transfer.

In addition, if the infrastructure of the acquired company is being integrated into that of the acquiring entity, a complete risk assessment of the infrastructure should be performed to determine if the security posture of the two infrastructures is compatible and to define which configuration changes or upgrades may be necessary to ensure the final system has a seamless security profile and no gaps exist.

**A complete iGaming solution often relies on several independent parties integrating with your site. Security responsibilities must be clearly defined for all external parties who are agreeing to access the same systems.**

The integration of third-party systems with iGaming platforms is an inevitable part of the architecture of these systems since various functions needed for the full operation of the iGaming system – identity verification, geolocation and payment processing – are often provided by third parties in addition to scenarios where game content may be provided by remote gaming servers. However, in order to minimize potential risks, the access of third parties to your systems must be clearly defined in any agreement with the third party, and the technical controls defining the communication protocols between the platforms must be carefully implemented. Testing of the Application programming Interface (API) security is advisable in most cases.

## Integrity Preventing interference in gaming processes

Maintaining integrity in the gaming process is a primary regulatory concern, and this is reflected in the focus of security regulations on controlling access to critical components of the iGaming system, such as the random number generator (RNG), the databases that store player information and gambling information, and the communication systems that link these different components of the iGaming platform together.

While the technical architecture of the iGaming platform is used to restrict access to critical components and the implementation of secure coding practices and communication protocols will provide the underlying basis for maintaining integrity in the iGaming system, internal controls and procedures also play an important role.



**Security threats can come from outside and within your business. A robust system of internal controls and security procedures simultaneously protects you, the business and your employees.**

Unfortunately, history has shown that threats to the integrity of gaming operations can come from internal sources as much as external sources. Maintaining integrity requires establishing a good system of internal controls which can:

- Provide management oversight
- Ensure accurate reporting
- Mitigate business risks
- Segregate work duties

Ensuring these controls are aligned with information security management requirements of a standard, such as ISO 27001, will improve the security posture of the organization.


## **Availability**

### **Ensuring access to gaming systems**

If the iGaming site is not available to players, then it cannot generate revenue. Improvements in the reliability of computer and network hardware and the use of virtualized redundant server clusters has increased the availability of complex computer systems enormously. However, systems still remain vulnerable to environmental threats and to operational threats. Operational threats result from human error in the operational processes surrounding the system infrastructure while environmental threats result from deliberate or uncontrollable events external to the online gambling system, in particular natural or man-made disasters and deliberate attacks against the online gaming system.

#### **Disaster Recovery Planning**

It can be costly to the iGaming operator in terms of lost revenue and reputation if there is an outage, whether temporary or long term, at the data center that is hosting an online gaming system. As part of the architectural design of the iGaming system, a secondary or backup site should be put in place to provide service in the event of a disaster, preventing access to the primary data centre.



**It is no secret that the world is experiencing an increase in the number of serious environmental catastrophes and geopolitical incidents. Disaster recovery planning must be an integral part of your operations.**

In an online gambling context, however, there is more to disaster recovery planning than simply having a second site available:

1. There must be complete mirroring between the two sites to prevent the loss of gambling data in the event of a disaster. While synchronized data transfer may be too costly to implement, a process offering almost real-time data updates with as small a recovery point objective as possible is needed.
2. The disaster recovery plan must be tested and exercised on a regular basis to ensure that the infrastructure is capable of supporting the disaster recovery process and that the technical staff at the online gambling operator is comfortable with executing the disaster recovery procedures.



## Distributed Denial of Service (DDoS) Attacks

Online gambling activities, such as sports betting, peer-to-peer games and live dealer games, occur in real time and are sensitive to service disruptions or transaction delays. A leading infrastructure provider reported that online gaming has remained the most targeted industry since Q2 2014, consistently being targeted in about 35% of DDoS attacks. In some cases, the DDoS attacks have been accompanied by extortion threats where the attacker has demanded a ransom in untraceable funds (such as bitcoin) to stop the attacks. While these attacks have been investigated by law enforcement authorities, gathering sufficient evidence to prosecute the attacking parties has proven difficult.

For the iGaming operator, a DDoS attack resulting in a service outage or disruption can lead to players abandoning play at a site or placing bets on other sites. Where ransom is the objective, DDoS attacks have been timed to coincide with large sporting events, increasing the potential losses to the targeted operator.



**The easy availability of cloud-based resources has enabled an increase in DDoS attacks with online gaming companies becoming a favorite target. DDoS mitigation must be part of your core security strategy.**

How can an iGaming operator protect themselves against a DDoS attack? There are three possible strategies:

1. An in-house solution using specialized hardware or software to filter and discard unwanted traffic. This approach suffers both from the fact that few businesses will have the bandwidth to cope with the traffic volumes in the first place, and the development of filtering software is both costly and uncertain depending on the security experience level of the development team.
2. Relying on a solution from an ISP provider. While ISPs may have more bandwidth available to them and may be able to spread the capital cost of filtering software across a number of customers, depending on their size, they may not have the expertise to manage such an attack.
3. Contracting a dedicated DDoS mitigation service. This approach involves using a cloud provider against the cloud-based attacker. These dedicated services have massive bandwidth and dedicated filtering software able to redirect unwanted traffic away from the target site.

The best strategy will depend on the risk assessment of the gaming operations and the business case for the level of protection necessary.

## SECURITY ASSESSMENTS AND AUDITS

The only way to ensure the correct functioning of an information security framework is to test it. Depending on the business requirements of the organization, testing can take a number of forms ranging from an assessment of the effectiveness of a particular information security framework element's effectiveness to a complete compliance audit of the information security system to achieve certification of the system.



An Information System Security Assessment is an evaluation of how well elements of the information security framework have been implemented in order to reveal areas of weakness or identify vulnerabilities and their impacts. Assessments are usually determined by specific business needs (e.g., a wireless security assessment may be requested to provide an independent assurance that a newly implemented wireless network has been configured properly and operates safely; a vulnerability assessment may be requested to verify that all of the servers on a particular network have been hardened according to their respective roles; penetration testing may be requested to provide assurance that web-facing applications are not vulnerable to attack from the Internet; etc.).

An assessment can also be performed on a similar set of controls to a published standard and the findings reported, but these findings would not confer a status of compliance or non-compliance.

An Information System Security Audit is an evaluation of how the information system security of an organization is implemented against a particular standard. The goal of an audit is to provide a determination of compliance. Compliance to a third-party standard may result in certification or accreditation to that standard. During an audit, any areas of non-compliance with the standard are brought to the attention of the audited organization in the form of non-conformance reports which must be addressed before a system can be deemed compliant.

An audit is the only way to formally establish that the requirements of a policy are being followed in practice. Audits may be performed internally or externally:

#### **Internal Audit**

An internal audit is conducted by designated staff members to determine if the organization is following the requirements laid down in its own corporate information security framework. Aside from making good business sense, the existence of an internal audit process is often a requirement for certification to a third-party information security standard.

#### **External Audit**

An external audit is conducted by a qualified, independent third party to determine if the organization's information security framework is compliant with a specific standard. Depending on the standard chosen and the auditing body, an external audit can lead to certification to a third-party information security standard.

An audit can be performed to only part or to the complete requirements of a published standard.

## **ASSESSMENTS VS AUDITS**

An Information System Security Audit is an evaluation of how the information security of an organization is implemented against a particular standard. This may be an evaluation against the organization's internal security policy and/or against an external security standard (e.g. ISO 27001:2005). The goal of an audit is to provide a determination of compliance.

An Information System Security Assessment is an evaluation of how well elements of the information security framework have been implemented in order to reveal areas of weakness or identify vulnerabilities and their impacts. The goal of an assessment is to provide a report on the assessment findings and make recommendations for improvement.

The difference between an "audit" and an "assessment" is that auditing is a measure of something against a specific standard, while an assessment measures how good or bad something is based on the expertise of the assessor and criteria agreed upon prior to the commencement of the engagement.

In both Security Audits and Security Assessments, the analysis can be performed against the technologies, people, and process applicable to information security within the organization. An assessment may take place before an audit in order to identify areas of improvement prior to an audit, or after an audit to investigate its effectiveness.

## Implementation Steps

Implementing a security information management program can seem like a daunting task. However, GLI's professionals have the expertise to assist iGaming operators in making the transition to implementing a robust information security management system that meets their specific needs based on the size of the organization, the markets in which it operates, and its particular technical solution.

## GLI's Services

### Audit

---

#### Information Security System Audit

To determine the security posture of an organization and its information systems and data, GLI conducts Information Security (INFOSEC) and security control assessments in accordance with worldwide, recognized procedures and guidelines.

#### Jurisdictional Information Security System Audit

GLI will perform an evaluation against specific gaming jurisdiction security standards and recognized security standards to determine how accurate and effective your implemented organization information security controls are.

#### ISO 27001 Information Security System Audit

We will evaluate your implemented organization information security controls against the ISO 27001 security standards to determine how accurate and effective they are.

#### PCI Qualified Security Audit

Qualified Security Assessor (QSA) companies are independent security organizations that have been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS. QSA employees are individuals who are employed by a QSA company and have satisfied, and continue to satisfy, all QSA requirements.

## **Personnel Security Audit**

Obtaining trustworthy personnel to operate and maintain critical information systems is of vital importance to the security posture of an organization. GLI evaluates and consults customers on personnel security programs that address security screening policies, personnel identification procedures, industrial security requirements, and security awareness training programs.

---

## **Physical Security Audit**

GLI performs extensive analysis and design of physical security control systems including: automated and manual entry control systems; facility monitoring equipment; intrusion detection systems; access control procedures; and other mechanisms designed to protect physical infrastructures. GLI has conducted physical security inspections for data centers, network operations centers (NOC), and security operations centers (SOC) throughout the world.

---

## **Continuity of Operations and Disaster Recovery Audit**

To ensure the availability of an organization's mission critical functions, GLI evaluates and consults on contingency plans and procedures, incident response plans, disaster recovery plans, and business impact assessments for major information systems, data centers, and worldwide telecommunication networks. The focus of these plans and procedures is to ensure continuity of operations and secure backup/recovery. We also evaluate specialized Continuity of Operations Plans (COOP) in accordance with specific agency guidelines and worldwide recognized Information Security standards.

---

## **Incident Management Audit**

Our review focuses on security incident management standards, guidelines and procedures as well as the implementation and governance of these activities. Security incident management may intersect or complement the help desk, problem management and operational incident reporting. However, this review focuses mainly on the security component.

---

## **Cloud Computing Security Audit**

Cloud computing is revolutionizing the information technology industry and the way that security is implemented. GLI is at the forefront of cloud computing security evaluating and consulting on cloud solutions security implementation.

---

## **Threat/Risk Management Analysis and Vulnerability Assessments**

An effective risk management program requires a thorough assessment of the threats to a particular information system as well as the vulnerabilities of the system to those threats. GLI provides customers with a comprehensive evaluation of the risk management implementation and analysis of naturally occurring and man-made threats to information systems using authoritative sources and various intelligence sources. These assessments are used to identify mitigation procedures and system modifications to close-known vulnerabilities, thereby enabling the information system to operate at an acceptable level of risk.

## Assessment

---

### Penetration Testing

GLI's penetration testing service will help companies determine weaknesses in their network, computer systems and applications. A standard penetration test might contain a vulnerability assessment through conventional system and software testing or network security scanning alone. Unlike other penetration testing companies who focus on assembly line assessments and automatic tools output, we take a different approach. GLI delivers a quality product tailored to your needs. We work with our customers to build an accurate profile of your primary business function, where threats come from, and your security assessment goals. This is done to ensure that the work conducted meets your exact needs and not just easily productized. We focus on long-term relationships with our clients to ensure they get the best penetration test possible, offering them high-end, professional security audit services developed for their needs.

### External Infrastructure Testing

External infrastructure assessments aim to answer the question, "Could an attacker compromise our Internet-facing resources?" External infrastructure testing explores the consequences of a hacker carrying out malicious activities from across the Internet. It involves surveying available network services, interrogating them for weaknesses, and trying to exploit them to extract information or compromise the network. GLI's methodology can be tailored to meet the requirements of PCI, ISO 27001 and gaming jurisdiction specifications. An external infrastructure assessment provides assurance that a network is safe from external threats.

### Internal Infrastructure Testing

Internal infrastructure assessments aim to identify "What could an attacker do if they had access to an organization's internal network?" Internal infrastructure testing is usually conducted at a client's premises and is often scenario and risk-based. An assessment could explore the consequences of a rogue employee or contractor carrying out malicious activities. It could involve trying to break into core company services from the guest Wi-Fi in the cafeteria. It can include reviews of standard desktop or laptop security as well as assessments of virtual local area networks (VLANs), VoIP, mobile and wireless networks. GLI's methodology can be tailored to meet the requirements of PCI, ISO 27001 and gaming jurisdiction specifications. Internal infrastructure assessments provide assurance that an internal network is safe from internal and external threats.

### PCI Approved Scanning Vendors quarterly scan

An ASV is an organization with a set of security services and tools ("ASV scan solution") to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2. The scanning vendor's ASV scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC's list of approved scanning vendors.



## Application Security Testing

An application security test is a method of assessing the security of an application (Web, compiled, mobile, etc.) and evaluating the effectiveness of controls that are implemented to protect the application and organization from risks posed by application-based flaws. Specifically, application security testing assesses application vulnerabilities that may jeopardize the confidentiality, integrity and availability of critical or sensitive data and establishes the priority to eliminate vulnerabilities or mitigate their potential impact to the organization. GLI application security testing helps an organization identify and remediate application-related vulnerabilities and flaws before hackers can exploit those vulnerabilities and flaws and gain access to the organization's systems, resources and confidential information. This service is flexible and can be tailored to meet specific client requirements. Our overall methodology is modeled after the Open Web Application Security Project (OWASP), an established guideline for comprehensive application security testing. OWASP is a worldwide free and open community focused on improving the security of applications. OWASP's mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks.

---

## Security Source Code Review

Security source code review is probably the single-most effective technique for identifying security flaws. When used together with automated tools and manual penetration testing, code review can significantly increase the cost effectiveness of an application security verification effort. GLI has reviewed source code for a variety of organization in the iGaming industry to verify that the proper security controls are present, work as intended, and have been invoked in all the right places. Code review is a way of ensuring that the application has been developed so as to be "self-defending" in its given environment and it is performed according to the OWASP open source framework.

---

## Social Engineering

GLI social engineers attempt, by personal contact, to steal your employees' confidential information by exploiting trust, good faith and helpfulness or through excessive demand and/or employee uncertainty. Depending on the test objective and target group, GLI uses different methods and types of social engineering attack.

---

## Consultancy

---

### Performance Monitoring

GLI can give you valuable insight into the speed and availability of your site and how it performs for your visitors. Core to GLI's website performance monitoring is our unique testing methodology and accurate, targeted alerting. As a result, we deliver the most reliable and consistent data on website performance available. The test is performed from outside your firewall, gaining a real user's view of your website's performance. Testing is consistent and repeatable - each test is throttled to simulate the end user connection speed. This means a realistic and consistent view of website speed without the interference of ISP connectivity.

## **Load Testing**

Load testing is an essential stage in the development lifecycle because it ensures that your site does not buckle under heavy load. GLI's user-friendly website load testing service allows you to control as much of the process as you wish. We offer tailored solutions based on your technical and business requirements. You can either manage your own tests with the Software as a Service (SaaS) option or opt for managed load testing and let our web performance assessors take the strain. To save time and money on unnecessary retests, it can be a good idea to carry out a pre-load test performance audit. This way, you can make sure your website is in the best possible shape to cope with extra load before you test it. Load testing is a recurring requirement. As we work with you to deliver your website load testing goals, we aim to transfer our knowledge to you so you can get the best out of our service for yourself. As we move through different projects, we can tailor our involvement to suit your requirements, ensuring that we always provide the level of support that you need.

---

## **ISO 27001 Gap Analysis**

Our experts can perform a gap analysis between the controls you currently have in place and those which would be required for compliance with ISO 27001. They will then work with you to develop a roadmap for implementing the controls which would make your governance processes compliant with ISO 27001.

---

## **Security Awareness and Training**

Security awareness and training is a vital component of any personnel security program. GLI develops a wide variety of security awareness and training curriculum, including general awareness training, information system specific training and security training for technical and developer personnel. GLI has authored numerous security awareness papers covering topics, such as the electronic intrusion threat, intrusion detection and response, security of Internet gaming IT systems, and certification and accreditation.

---

## **Organizational Key Processes Evaluation**

GLI provides an in-depth consultancy service in relation to key organizational processes, such as System Development Life Cycle (SDLC), change management, IT governance, project management, etc., aiming to advise organizations on how to streamline those processes while eliminating the waste and adopting effective solutions.

---

## **Disaster Recovery Consultation**

GLI leverages its many years of experience in providing disaster recovery auditing and assessment services. GLI's experts can advise on disaster recovery strategies and assist in the planning and execution of disaster recovery testing.

## About GLI

Gaming Laboratories International (GLI®) is the world's leading land-based, iGaming and lottery testing laboratory.

For 26 years, Gaming Laboratories International, LLC has continuously delivered the highest quality land-based, lottery and iGaming testing and assessment services with supreme accuracy while reducing time to market.

With over 20 laboratory locations spread across Africa, Asia, Australia, the Caribbean, Europe, North America and South America, GLI holds U.S. and international accreditations for compliance with ISO/IEC 17025, 17020, and 17065 standards for technical competence in the gaming, wagering and lottery industries.

### GLI's Professional Services Qualifications:

- Certified Quality Software Engineer (CSQE)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Security Manager (CISM)
- Certified Information Security Auditor (CISA)
- ISO 27001 Lead Auditor (LA)
- Payment Card Industry Qualified Security Assessor (QSA)
- Payment Card Industry Professional (PCIP)
- Certified Quality Software Engineer (CSQE)
- Certified Ethical Hacker (CEH)

### FOR MORE INFORMATION

For more information on the services offered by GLI, please visit [www.gaminglabs.com](http://www.gaminglabs.com).

### REQUEST A CALL

To request a call or to ask a question, contact one of GLI's North American office locations listed. A GLI representative will respond to your inquiry within two business days.

## GLI OFFICE LOCATIONS:

### Global Headquarters

600 Airport Road  
Lakewood, NJ 08701  
Phone: +1 (732) 942 3999  
Fax: +1 (732) 942 0043

### Las Vegas Office

7160 Amigo Street  
Las Vegas, NV 89119  
Phone: +1 (702) 914 2220  
Fax: +1 (702) 914 2799

### Colorado Office

4720 Independence Street  
Wheat Ridge, CO 80033  
Phone: +1 (303) 277 1172  
Fax: +1 (303) 277 9901

**GLI Canada** British Columbia  
Office Suite 210 – 6400 Roberts Street  
Burnaby, BC V5G 4C9

Phone: +1 (778) 331 0794  
Fax: +1 (778) 331 0799

**GLI Canada** New Brunswick  
Office Suite 130 – 11 Ocean Limited Way  
Moncton, NB E1C 0H1

Phone: +1 (506) 855 0214

### GLI Europe BV

Satellietbaan 12  
2181 MH  
Hillegom, The Netherlands  
Phone: +31 (0) 252 529 838  
Fax: +31 (0) 252 529 608