GLI'S PROPOSAL

IN RESPONSE TO

THE MARYLAND LOTTERY AND GAMING CONTROL AGENCY

REQUEST FOR PROPOSAL

FOR

ANNUAL NETWORK RISK ASSESSMENT SERVICES

JULY 6, 2015

SUBMITTED BY

GAMING LABORATORIES INTERNATIONAL, LLC

Table of Contents

Cover Letter iii
ABOUT GLI 4
PROJECT TEAM EXPERIENCE 5
PRIOR EXPERIENCES & REFERENCES 14
APPROACH AND METHODOLOGY 20

COVER LETTER

July 6, 2015

Mr. Charles LaBoy, CPA
Assistant Director of Gaming
Maryland Lottery and Gaming Control Agency
1800 Washington Blvd, Suite 330
Baltimore, MD 21230

Re: ***Annual Network Risk Assessment Services***

Dear Mr. LaBoy:

Gaming Laboratories International, LLC (GLI) is pleased to submit this proposal indicating that we would like to be an approved entity with the Maryland Lottery and Gaming Control Agency (MLGCA) to provide network risk assessment services for the MLGCA and the casinos in the State of Maryland. In this proposal, GLI will demonstrate that we possess the requisite competency and experience to successfully perform all of the functions described in this RFP.

GLI's Professional Services Division has been providing Network Risk Assessment, Information Security Consulting and other Professional Services to a vast number of gaming commissions, lotteries and casinos over the years. Furthermore, we currently have a contract with the Maryland Department of Information Technology to provide consulting and technical services for the State.

I, James Maida, as President of Gaming Laboratories International, LLC, am legally able to commit the firm to enter into a contractual relationship with the MLGCA, and commit the firm to perform the tasks and submit deliverables.

On behalf of our outstanding professionals, GLI looks forward to your evaluation of our proposal. This submission demonstrates our commitment in providing the MLGCA with the highest quality of service. Should you have any questions or require additional information regarding GLI's submission, please contact Bill Higgins, Senior Manager Professional Services, at 506-961-5566.

Sincerely,

James R. Maida
President

ABOUT GLI

GLI's Professional Services Division has been providing Network Risk Assessment, Information Security Consulting, and Professional Services to a number of industries over the past several years. In particular, specific Information Technology services that we provide include (but are not limited to):

- Network risk assessments including vulnerability assessment and penetration testing
- Network infrastructure assessments
- IT security auditing against the appropriate Security Standards such as ISO 27001
- Risk assessments
- PCI services

GLI has been providing testing and consulting services to the gaming industry for over twenty-five years. We provide complete independent testing and certification services for all types of gaming systems and equipment. This includes gaming devices in casinos such as protocol analysis and certification, amusement games, progressive systems/signs, tote systems at pari-mutuel facilities, gaming device peripherals (bill validator, printers, card readers, etc.), video lottery, central system testing and certification, cashless wagering systems, and sports betting. We also serve as an independent consultant to governments in the development of rules and regulations and technical specifications relating to casino gaming.

GLI operates 12 fully accredited testing laboratories worldwide, five fully accredited inspection bodies in America, Europe and Africa, and two fully accredited product certification bodies in the U.S. and Netherlands. GLI is the only independent testing laboratory of its kind to retain U.S. and International accreditations for compliance with ISO 17025 and Guide 65 standards for technical competence in testing, inspection, and product certification services.

At GLI, the employees are constantly focused on meeting the demands of its clients with integrity, accuracy and efficiency. Our independence, adherence to strict ethical standards, commitment to quality and 24-hour 365-day per year customer support are only part of what makes us so unique that we have earned the trust and confidence of clients throughout the world.

In order to deliver this level of service in the face of the demands imposed on our clients by the escalating introduction of new technology, we continue to invest in our workforce, capital facilities, training, new technological tools and more efficient means of communicating information. The result is a worldwide staff of more than 800 professionals working at 21 offices on six continents working not only to advance the science of testing gaming and lottery equipment, but working to advance the science of service as well.

PROJECT TEAM EXPERIENCE

GLI is pleased to present a very experienced team to work with MLGCA and the various properties throughout the state. GLI team members have a combined 80+ years of experience working or serving clients in this field. This experience will enable our team members to complete this engagement more efficiently, while using less of your organization personnel's time, resulting in less cost and time for your organization. You will not have to invest any of your time or money educating our team members. ***GLI attests that the qualifications of its proposed professionals will exceed the requirements and experience requisite to perform the services requested.***

GLI's team of professionals hold the following industry recognized certifications:

- Certified Chief Information Security Officer (CCISO)
- EC Council Certified Ethical Hacker (CEH)
- Certified Penetration Tester (CPT)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- ISO 27001 Lead Auditor
- Accredited World Lottery Association Security Control Standard Auditor
- Payment Card Industry Qualified Security Assessor (PCI-QSA)
- Project Management Professional (PMP)

Project Team Members

Name	Role	Job Description
Thomas Bierbach	Engagement Manager	Thomas will be responsible for high-level project oversight and project management to ensure that all stakeholders' business needs are met, such as deadline and budget requirements. He will provide technical advice to team members on any phase of the project required as well as perform reviews of the work in progress to ensure that quality assurance standards are being met.
Rob Lavin	Technical Manager	Rob will be responsible for leading the audit of any system security controls over the network deemed critical (the vulnerability assessments and penetration testing).
Cory Johnson	ISS Senior Auditor	Cory will work closely with Rob Lavin in the delivery of the fieldwork and testing requirements of this assessment.
Garret Ronning	ISS Auditor	Garrett will work closely with Rob Lavin in the delivery of the fieldwork and testing requirements of this assessment.
James Smith	ISS Auditor	James will work closely with Rob Lavin in the delivery of the fieldwork and testing requirements of this assessment.

RESUMES

THOMAS BIERBACH
CISA, CISM
ENGAGEMENT MANAGER

Mr. Thomas Bierbach is a consummate professional in the field of Lottery Risk Management and Security & Compliance, working with organizations in the identification and implementation of Security & Compliance programs in support of operational integrity, fraud prevention and player protection. Thomas has held senior roles in Risk Management in the lottery industry, such as the Director of Security & Compliance at Atlantic Lottery, supported lotteries in creating the competitive edge of a world class organization while maintaining highest standards of Security and Integrity. Having represented Canada as Co-Chair on the World Lottery Association Security & Risk Management Committee (WLA SRMC), supporting development of and propagating WLA Security Control Standard, Thomas brings a broad global perspective to the team.

Thomas is an accredited WLA Security Control Standard Auditor and Certified ISO 27001 Lead Auditor and has led Lotteries through ISO/IEC 27001 implementation and certification as well as WLA Security Control Standard Certifications. As experienced and Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA) with over 20 years of international technology and management experience, he is a leader in lottery security.

PROJECT ROLE

Thomas will be responsible for high-level project oversight and project management to ensure that all stakeholders' business needs are met, such as deadline and budget requirements.

He will perform reviews of the work in progress to ensure that quality assurance standards are being met.

CREDENTIALS

- CISA
- CISM
- Certified ISO 27001 Lead Auditor
- Accredited WLA Security Control Standard Auditor

Professional Experience

Senior Manager, Professional Services – GLI Professional Services (2015 – Present)
Providing cross-disciplinary business development, management and service delivery to GLI Professional Services for WLA SCS© (World Lottery Association - Security Control Standard) and ISO 27001 information security management systems certification audit services as well as lottery security and integrity services. Management and execution of global business development in domestic and international markets and providing technical sales support to the global GLI sales teams.

Senior Consultant - Atlantic Lottery Professional Services (2014 – 2015)
Advisor to development of professional services practice for lottery and gaming industry. Provision of Lottery Risk and Security subject matter expertise in consulting and WLA Security Control Standard SCS Certification projects.

Director of Lottery Security & Audit Services – BMM Testlabs (9/2012 – 1/2014)
Acted as a Senior Advisor in the development and delivery of products and services for Lottery & Gaming Security and Compliance Management, including Lottery Security Assessments and the Design and Implementation of Controls and Fraud Detection and Compliance Programs.

Vice President, Risk Advisory and Compliance – Baseline Business Geographics Inc. (2011 – 10/2012)
Provided Risk Management and Security & Compliance advisory services in the Gaming and Lottery industry, working with organizations in the identification and implementation of security & compliance programs and solutions in support of player protection and operational excellence. Oversaw the market and brand development for Baseline's GIS/GPS and mobile technology supported Site Compliance & Inspection solutions.

Vice Chair WLA Security & Risk Management Committee – World Lottery Association (WLA) (2008 – 2011)
Built worldwide industry and cross jurisdictional relationships and liaisons within the Gaming and Lottery Industry, presented on security issues on a global stage, and contributed to the evolution of the international WLA Security Control Standard.

Director Security & Compliance - Atlantic Lottery Corporation (2007 – 2011)
Lead the development and management of programs, processes and services to ensure the integrity of lottery products and processes, the security of corporate assets, the protection of players and the regulatory compliance of the lottery operations.

Manager, IT Audit – Atlantic Lottery Corporation (2005 – 2007)
Providing assurance to management and stakeholders that risks are appropriately managed, presenting position on risk and significant issues to all levels of management and promoting change supporting the organization in meeting its objectives.

Operations Manager – Intelisys Aviation Systems (2000 –2005)
Management of systems and production group, coordination of quality assurance, policies and procedures, process development and improvement and business continuity planning. Enforced high availability standards within the production data centre and mission critical operations of ASP delivery of aviation SW to midsize and regional airlines.

ROB LAVIN
C/CISO, CPT, CEH
TECHNICAL MANAGER

As a Manager of GLI Professional Services, Rob Lavin leads a dedicated professional services business line that includes Vulnerability/Penetration Assessments, Information Security Systems (ISS) Assessments and Process Improvement Advisory Services.

Rob has over 20 years experience in both private and public sectors managing information systems. Prior to joining GLI, Rob served as Senior Security Architect Consultant for the Office of Chief Information Officer Government of Newfoundland and Labrador, where he designed and implemented processes that ensured continual forward movement of the government information technology revitalization strategy.

Rob has recently completed security audits for the California State Lottery, Rhode Island Lottery, Atlantic Lottery Corporation, Alberta Gaming and Liquor Commission, Colorado Lottery, Ontario Lottery and Gaming, and the Western Canada Lottery Corporation.

PROJECT ROLE

Rob will be responsible for leading the audit of any system security controls over the network deemed critical (the vulnerability assessments and penetration testing).

CREDENTIALS

- Bachelor of Arts, Saint Mary's University
- ISO 27001 Certified Lead Auditor
- Certified Chief Information Systems Officer (C/CISO)
- Certified Penetration Tester (CPT)
- Certified Ethical Hacker (CEH)

Professional Experience

Manager, Professional Services and IS Auditor (8/2012 – Present)
Responsible for leading and executing professional services including Governance, Risk and Compliance, ISO 27001 certification, Project Management and Security consultant, specializing in network security architecture, vulnerability assessment and penetration testing for gaming networks to comply with World Lottery Association best practice for security controls.

Senior Security Consultant & CSO - Nival Group Inc. (6/2011 – 8/2012)
Directed development and design of professional services related to Internet/information security and broadband consulting, identified emerging technology security issues, developed corporate security programs, security audits, vulnerability and penetration assessments, and performed the duties of a Virtual CSO.

Senior Security Architect (Contract) - Government of Newfoundland & Labrador CIO office (2/2012- 6/2012)
Designed and implemented processes that ensured continual movement from the current security state to the future state, closed gaps between government strategy and the ability of the IT security dimensions to support the strategy, identified protection goals, objectives and metrics consistent with corporate strategic plan, and managed the development and implementation of global security policy, standards and procedures.

Manager of IT/CSO - Medavie EMS (11/2006 – 5/2011)
Responsible for security, management and coordination of daily IT operations, managed the operational and capital budget, technology for the 7x24 EHS ambulance communication dispatch centre and backup site, liaised with vendors, contractors and external consulting agencies and co-authored a comprehensive Business Case for Medavie EMS, co-managed the end-to-end process from Business Case recommendations and approvals, to RFP development, vendor response reviews, short list interviews, final recommendation and approvals.

Manager of IT/CSO - Thor Solutions Inc. (5/2000 – 11/2006)
Directed development and design of managed services related to Internet security and broadband consulting, completed application development, infrastructure (wireless/wired) rollouts, and security upgrades, managed numerous Security Audits which included, VA's, PEN test, and TRA's, oversaw incident response planning and investigation of security breaches, and assisted with disciplinary and legal matters associated with such breaches.

Instructor - Dalhousie University (4/1991 – 4/2007)
Developed and delivered technology courses (Intro to LAN and Security; Hands on Information Security) to a diverse audience: beginners to knowledgeable IT individuals, customized and delivered training to the RCMP high tech crime unit and was guest speaker on Internet Crime and Protect for the Halifax Police, as well as numerous international conferences on topics ranging from risk assessment to cloud computing security.

Senior Network/Security Architect / Team Lead - Nova Scotia Power (5/1990 – 5/2000)
Provided E-Commerce and Network Security solutions Nova Scotia Power, managed annual project budgets in excess of $2M and operational/capital budgets of over $750K, developed service level agreements and managed public tendering and contracting functions and was Project Manager for the Y2K project and data network upgrade from ATM to Gigabit.

CORY JOHNSON
CISA, PCI QSA, SECURITY+
ISS SENIOR AUDITOR

Cory is an ISO 27001 Lead Auditor and penetration tester, having developed a broad range of experience in government, public and private industry. As a Testing Engineer, penetration tester and Information security auditor, Cory brings an in-depth knowledge of gaming and lotteries along with their specific associated information security risks.

Being a Certified Information Systems Auditor (CISA), Cory has lead information security governance programs based on ISO 27001. Cory is an experienced internal audit leader, having implemented audit programs designed to evaluate and resolve complex internal control and operational problems in the lottery, iGaming and Casino Information Systems sectors. He has delivered WLASCS/ISO 27001 certification audits to many North American lotteries, audits against the ISO 27001 standards to iGaming providers in both North America and Europe, and penetration tests for numerous casinos in the U.S.

Cory has conducted over 50 Information Security audits in 12 U.S. states and 7 countries.

PROJECT ROLE

Cory will work closely with the **Technical Manager in the delivery of the fieldwork and testing requirements of this assessment.**

CREDENTIALS

- ISO 27001 Certified Lead Auditor
- Certified Information Systems Auditor (CISA)
- PCI QSA
- Security +

Professional Experience

Test Engineer Level II - GLI (2008 – Current)
Responsible for testing kiosks and casino slot accounting systems against Jurisdictional regulations. Develop new testing strategies to find and isolate potential problems, troubleshoot and identify operational problems in gaming apparatus. Conduct vulnerability and penetration testing, as well as information systems process auditing (ISMS) and software security analysis.

IT Manager – Redneck Concrete (2005 – 2008)
Responsible for the management of infrastructure for the company, including telecommunications, radio repeater equipment, as well as software licensing, Maintenance of the accounting system. Also managed business continuity and disaster recovery.

GARRETT RONNING
ISS AUDITOR

Garrett will act as IT Security under Mr. Bierbach, supporting completion of this assessment. Having a broad IT background working in the gaming industry, Mr. Ronning has performed many roles from Network and Systems Administrator to System Security Specialist and Tech Support.

Garrett possesses an NSA certified degree in Information System Security and certifications in Computer and Communication Security, Microsoft Network Administration and Security, and as a Computer Networking and Information System Security Professional.

PROJECT ROLE

Garrett will work closely with the team in the delivery of the fieldwork and testing requirements of this assessment.

CREDENTIALS

- Computer and Communications Security
- Microsoft Network Administration and Security
- Computer Networking and Information System Security Professional

Professional Experience

ISS Auditor - GLI (12/2011 – Present)
Responsible for participating in audits on the Information Systems of clients to evaluate whether they comply with the requirements as set by the regulator and/or to ISO, PCI or other relevant standards, as well as for audit planning, field work documentation and contributing to audit reports.

IT Administrator - Little Creek Casino (12/2011 – 12/2014)
Responsible for the delivery of value-add advisory services that include Governance, Risk and Compliance (GRC), and Technical Services, and for providing consulting services for the implementation of information security programs, risk assessments, compliance reviews, and outsourcing advisory services.

Civil Engineering Technician – Hatton Godat Pantier (9/2004 – 3/2008)
Designed housing developments, including: overall grading, water, sewer & drainage systems designs, pond sizing calculations. Worked with MicroStation V8, Inroads, AutoCAD, Rhino 3D and many other drafting and design programs. Worked in a team environment to complete projects.

JAMES SMITH
ISS AUDITOR

James has a background in penetration testing, corporate forensic fraud investigations, IT auditing, and network administration. Having presented at top security conferences, James has also participated in hacking competitions, having placed in the top three at the HTCIA conference in September 2014.

As a trained penetration tester, James has conducted information security audits within large international environments, developed an automated platform which provides targeted geospatial threat analysis and has developed a broad range of experience in government, public and private industry.

PROJECT ROLE

James will work closely with the team in the delivery of the fieldwork and testing requirements of this assessment.

CREDENTIALS

- Certified Ethical Hacker (CEH)
- Security +

Professional Experience

Information Systems Security Auditor - SLI (02/2014 – Present)
Responsible for performing Penetrating Testing, Network Infrastructure and Web Application Vulnerability Assessments all while staying on top of the latest trends in cyber security.

Backbone Engineer Tier 3 – Innovatia (07/2012 – 02/2014)
Responsible for supporting media servers (S8xxx), H.248 media gateways (G450, G430, G350), Port Networks (G650, MCC, SCC), IP (H.323 and SIP), DCP phones and a host of network protocols (ISDN, QSIG, T1, E1). Delivered training and supporting Level 2 support associates as well as troubleshooting customer issues.

Data Operator – Bell Aliant (07/2011 – 11/2011)
Responsible for tape management, server installation/removal, circuit installation, and to monitor systems and equipment located at the data centre.

Threat Analyst & Canada Desk Chief – Project Vigilant LLC (02/2011 – 01/2014)
Responsible for establishing data analytics for information security metrics management, build metrics with directional, diagnostic and historical trending and establish cyber intelligence and counterintelligence programs leveraging existing and open source tools. Also conducted OSINT investigations.

Independent Penetration Tester – SmithwaySecurity (11/2010 – 02/2014)
Conducted vulnerability assessments and penetration testing for a variety of clients including financial institutions and government agencies via manual and verification exploration.

PRIOR EXPERIENCES & REFERENCES

As the summary below will illustrate, over the past few years GLI has been:

- Growing and capturing market shares in the security assessment space;
- Delivering quality service as demonstrated by the level of repeat business;
- Expanding rapidly in the network risk assessment services due to GLI's very strong background in security;
- Delivering quality as demonstrated by the expansion into different areas with the same clients; and
- Signing long term contracts with clients due to the quality of its work and deliverables, including the Maryland Department of Information Technology.

Network Risk Assessments & Penetration Testing 2012 - 2015

- 888 Holdings
- Alberta Gaming and Liquor Commission
- Aqua Caliente Gaming Commission
- Bally Interactive
- Cache Creek Casino
- California State Lottery
- Cliff Castle Casino
- Comanche Nation Gaming Commission
- Condado Plaza Hotel & Casino
- El San Juan Hotel & Casino
- Eastern Shoshone Gaming Agency
- Graton Resort and Casino
- Gun Lake Gaming Commission
- Habematolel Pomo of Upper Lake
- Iowa Racing and Gaming Commission
- Lake of the Torches Casinos
- Mille Lacs Band of Ojibwe Indians
- Pauma Gaming Commission
- Prairie's Edge Casino
- SHFL Entertainment
- Squaxin Island Gaming Commission
- Sycuan Casino Resort
- Tropical Casino Bayamon PR
- Upper Sioux Commission

Security Assessment Engagements

- AGLC 2013
- Atlantic Lottery Corporation – 2011/2012/2013/2014/2015
- California State Lottery – 2011/2013/2014/2015
- Hoosier Lottery (Indiana) – 2011/2013

- Loto-Quebec – 2011/2012/2013/2014/2015
- Ontario Lottery and Gaming Corporation – 2013/2014
- Rhode Island Lottery – 2013/2014/2015

Other Gaming Industry Engagements

- Alberta Gaming & Liquor Corporation (AGLC) Project Audit – 2013
- Alberta Gaming & Liquor Corporation (AGLC) Video Lottery Network Security Assessment – 2013
- Atlantic Lottery DRP Assessment – 2012
- Atlantic Lottery Project Audit – 2011
- Atlantic Lottery VLT Project Management – 2011/2012/2013/2014
- California Lottery WLASCS & ISO 27001 Training – 2013
- Oregon Lottery Project Audit – 2011
- Oregon VLT Project Management – 2013/2014

GLI is pleased to provide the following four (4) references for completed projects similar to the scope of services requested by MLGCA:

No.	Reference	Description of Work
1	**Company:** Eastern Shoshone Gaming Commission **Engagement:** Network Risk Assessment **Date:** June 2014 **Contact Name:** Cassandra Burnett **Title:** Vice Chair **Phone Number:** 1-307-335-8200 **E-mail:** cassaundraburnett@yahoo.com	The Eastern Shoshone Gaming Commission requested that GLI perform the following services at two of their casino properties: • Internal Network Assessment • External Network Assessment • Wireless Network Assessment Internal Network Risk Assessment: GLI's team performed an Internal Network Risk Assessment which enabled us to identify possible vulnerabilities or holes in the network that a potential hacker or a malicious employee might use to take the system down or worse, plant possible viruses on the system that would enable a person to steal or manipulate the income of the property. GLI gathered all possible known vulnerabilities against a published vulnerabilities database and scanned all ports for possible areas that will help a hacker gain access to the property network. External Network Risk Assessment: This vulnerability assessment was conducted off-site remotely. GLI performed a port scan of supplied IP addresses, followed by an attempt to exploit any vulnerabilities found. No exploits were attempted that either: a. were known to cause a Denial of Service. b. were known to be non-reversible or would leave the affected devices more open to unauthorized attack than they were when GLI started. Wireless Network Risk Assessment: This assessment completely mapped all wireless access points that were on the property at the time of the assessment and reviewed the network to determine if there were any access points that were on the network that were not authorized to be there. GLI identified the encryption levels and the risks involved in the encryption levels found and identified how far the wireless bled outside of the property to prevent possible hackers from being outside the casino and attempt to hack the system. All areas of vulnerabilities that were indentified were included in our in-depth report.

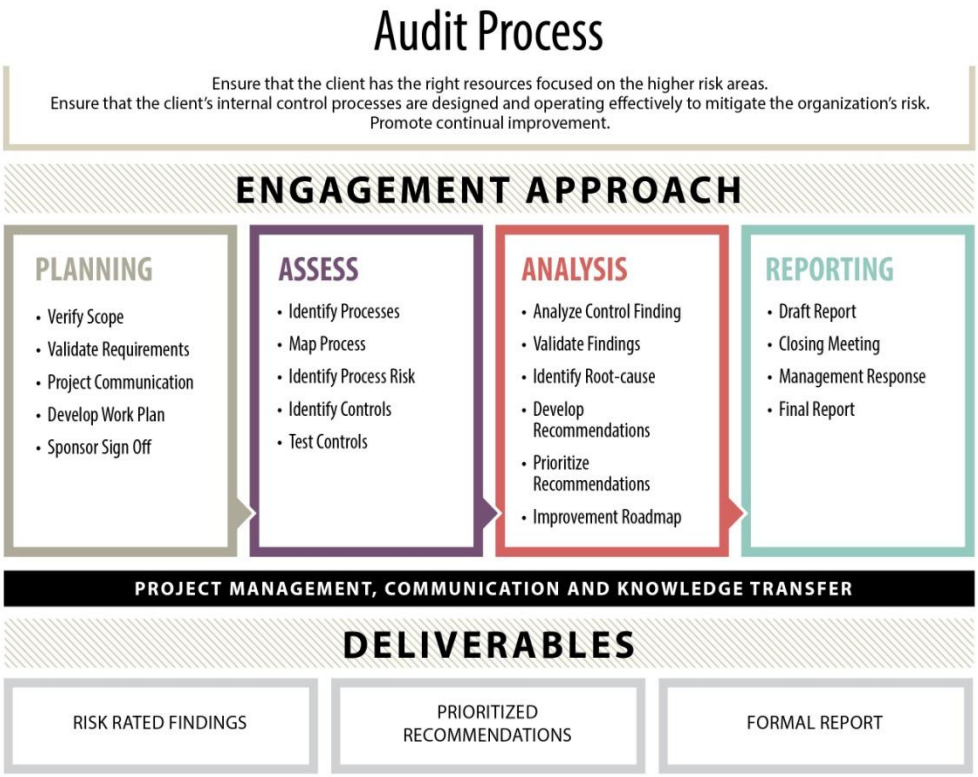
No.	Reference	Description of Work
2	**Company:** Pauma Gaming Commission **Engagement:** Network Risk Assessment **Date:** January 2015 **Contact Name:** Alex Sanchez **Title:** Executive Director **Phone Number:** 1-760-742-1020 **E-mail:** asanchez@paumatga.com	The Pauma Gaming Commission requested that GLI perform the following services at their casino properties: • Internal Network Assessment • Wireless Network Assessment Internal Network Risk Assessment: GLI's team performed an Internal Network Risk Assessment which enabled us to identify possible vulnerabilities or holes in the network that a potential hacker or a malicious employee might use to take the system down or worse, plant possible viruses on the system that would enable a person to steal or manipulate the income of the property. GLI gathered all possible known vulnerabilities against a published vulnerabilities database and scanned all ports for possible areas that will help a hacker gain access to the property network. Wireless Network Risk Assessment: This assessment completely mapped all wireless access points that were on the property at the time of the assessment and reviewed the network to determine if there were any access points that were on the network that were not authorized to be there. GLI identified the encryption levels and the risks involved in the encryption levels found and identified how far the wireless bled outside of the property to prevent possible hackers from being outside the casino and attempt to hack the system. All areas of vulnerabilities that were indentified were included in our in-depth report.

No.	Reference	Description of Work
3	**Company:** Alberta Gaming and Liquor Commission **Engagement:** Security Review **Date:** June 2013 to August 2013 **Contact Name:** Gordon Skingley **Title:** Manager Information Security **Phone Number:** 1-780-577-6912 **E-mail:** gordon.skingley@aglc.ca	GLI is pleased to have been engaged to provide a security review of the infrastructure associated with the new VLT deployment in Alberta. The overall objective was to conduct a comprehensive review of the Alberta Gaming and Liquor Commission (AGLC) Network and its Video Lottery (VL) Gaming Network. The review assessed the security measures which support the integrity, and security posture of the AGLC Lottery operations, computer security, and system security. We utilized a risk-based approach in conducting the lottery security audit. GLI reviewed documentation regarding the network design and interviewed network architects to clarify any questions on the design. In addition, we accessed the current design structure of various control mechanisms in place to determine their effectiveness. Our engagement included (but was not necessarily limited to) assessments of the following: ✓ Active Directory and Logical Access Configuration ✓ Antivirus ✓ Firewall and Devices Security ✓ G2S Protocol Security ✓ Intelligen Security Configuration and Server Hardening ✓ Intrusion Detection/Prevention ✓ Network IP Address Mapping ✓ Network Monitoring ✓ Penetration Testing ✓ Primary and Secondary DC & Multi Site Physical and Environmental Security ✓ Remote Access - VPN Architecture ✓ VL Network Architecture ✓ VLT Retailer Site Vulnerability Assessment ✓ VLT System Equipment Vulnerability Assessment

No.	Reference	Description of Work
4	**Company:** California State Lottery (CSL) **Engagement:** Security Assessments **Date:** 2012/2013/2014/2015 **Contact Name:** Mr. Roberto Zavala **Title:** Chief Executive, Internal Audits **Phone Number:** 1-800-568-8379 **E-mail:** rzavala@calottery.com	The overall purpose of these engagements was to conduct a comprehensive review of all aspects of lottery security in accordance with the Lottery Act of 1984, section 8880.46. The audits assessed the security measures that support the integrity, honesty and fairness of CSL's operations, computer security, and system security. Our assessments were conducted using a risk-based methodology to determine security control risk by evaluating the criteria of likelihood and impact of the risk event occurring. The audits reviewed the information security management processes for compliance against the Lottery Act of 1984, section 8880.46 and considered compliance to WLASCS 2006 & ISO 27001 standards. The certification audits included the following: Information Security Management Framework: 1. Organizational Structure 2. Asset Identification 3. Risk Assessment Methodology 4. Control Selection and Implementation 5. Management Process and Documentation 6. Resource Management 7. Training and Awareness 8. Internal Audit 9. Management Review 10. Continual Improvement The audits also covered the various ISO 27001 controls selected by CSL to mitigate risk to gaming systems assets: 1. Security policy 2. Organization of information security 3. Asset management 4. Human resources security 5. Physical and environmental security 6. Communications and operations management 7. Access control 8. Information systems acquisition, development and maintenance 9. Information security incident management 10. Business continuity management 11. Compliance Vulnerability scan assessments of the wired and wireless network were also performed.

APPROACH AND METHODOLOGY

GLI's team will utilize standard assessment methodology for this engagement as outlined in the graphic below which provides a high-level depiction of the activities within each phase of the engagement. The GLI assessment process is comprised of four phases: planning, assessment, analysis and reporting. This four phase system delivers an effective, efficient and quality product.



GLI's Network Risk Assessment (NRA) Methodology

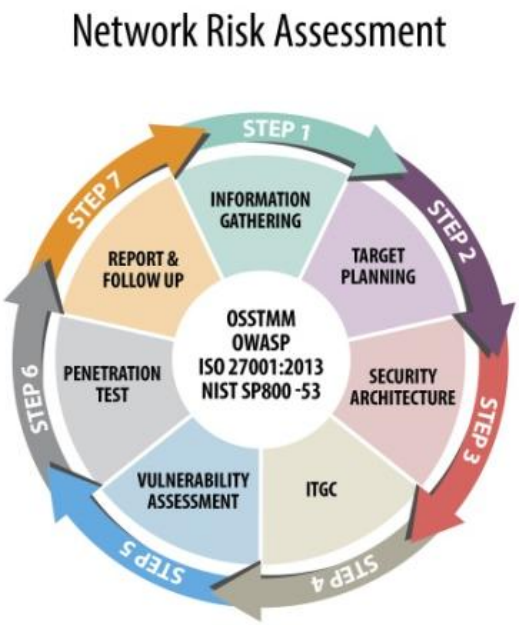


Exhibit: Network Risk Assessment (NRA). *The above model represents GLI's Seven Step Process for performing Network Risk Assessments to identify security vulnerabilities.*

GLI utilizes standardized vulnerability assessment and penetration testing methodology as prescribed by The Open Source Security Testing Methodology Manual (OSSTMM), and the Open Web Application Security Project (OWASP).

GLI uses a variety of commercial and freeware tools supplemented by manual verification of findings by its experts. Our inventory of tools is continuously expanded and updated.

GLI's NRA methodology will ensure that information gathered throughout the assessment process will be of sufficient detail to accurately assess the areas of risk exposure and their potential impact on the operating environment. The results of our security audit will identify for management those areas in the operations where improvement should be considered, and recommend strategies for improving those areas.

GLI's security auditors believe in the practice of Defense in Depth, an Information Assurance concept the uses multiple layers (depth) of security controls (defense) throughout an information technology (IT) system. The intent of this concept is to provide an IT system security redundancy. In the event of the failure of a system security control or in the event of an exploitation of system vulnerability, the system is better protected because there are multiple layers of security.

As a result, GLI views security as a framework of processes and tools working together to protect your most critical assets. This concept will include:

- Information Security Management System
- Process Implementation Compliant with ISO 27001
- Perimeter Firewalls

- Intrusion Prevention and Detection System – external and internal
- The use of segregated network zones
- Use of subnets through router or switch control
- Proper patch and change management for systems
- Proper use of roles based access
- Redundancy of servers and backup of critical data
- Physical and environmental review
- Incident Management
- Disaster Recovery Planning/Business Continuity Management

Critical Focus Areas to Consider

Privileged Account Monitoring	• The monitoring of the use of privileged user accounts within network and gaming systems.
IT Change Monitoring	• The management and enforcement of IT Changes across networks systems.
Firewall & VPN Monitoring	• The management and enforcement of security policies across firewalls, routers, virtual private networks (VPNs), and related security devices.
Intrusion Detection & Prevention	• Intrusion prevention and detection systems , are network security appliances that monitor network and/or system activities for malicious activity.
Log Monitoring / Security information management (SIM)	• Provides a system for collecting, storing, analyzing and querying log, threat, vulnerability and risk related data.
Vulnerability Assessment	• A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system
Penetration Testing	• A penetration test, is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders.
Social Engineering	• Social engineering, in the context of security, is understood to mean the art of manipulating people into performing actions or divulging confidential information.

External Network Risk Assessment Process

This vulnerability assessment will be conducted off-site remotely. GLI will perform a port scan of supplied IP addresses, followed by an attempt to exploit any vulnerabilities found. No exploits will be attempted that either:

- are known to cause a denial of service
- are known to be non-reversible or will leave the affected devices more open to unauthorized attack than they were when GLI started

The External Network Assessment will include the following:

- verifying the integrity of designated external firewalls against external attack

The port scan may be performed from multiple locations and multiple source IPs. If incident detection assessments are desired, the source IPs can be disclosed when GLI is on-site.

- ARIN search of the domain addresses to see what leased blocks they belong to
- Research the above information for possible user names/passwords if brute forcing becomes necessary
- Scan of the IP addresses
- Attempt to gain access via discovered vulnerabilities
- Brute force any services/web portals if possible
- SQL injection tests if necessary
- Verify the security of outward facing services allowed by the firewalls
- Enumerate and/or scan what is on the other side of any firewalls if sufficient access/information is acquired

External Penetration Assessment: The GLI team will perform an External Penetration Assessment. This will enable us to validate the vulnerabilities found during GLI's vulnerability scanning.

The penetration test is a method of evaluating the security of your computer systems and/or network by simulating an attacker. This process involves an active analysis of your system for any weaknesses, flaws or vulnerabilities. The analysis is performed from a potential attacker's position and can involve active exploitation of the security vulnerabilities discovered during the vulnerability scans.

Unlike the vulnerability scans, the penetration testing is mainly a manual process. GLI will manually probe the target host for common mis-configurations or flaws because a vulnerability scanner can fail to identify certain vulnerabilities.

Internal Network Risk Assessment Process

GLI's team will perform an Internal Network Risk Assessment. This will enable us to identify possible vulnerabilities or holes in the network that a potential hacker or a malicious employee might use to take the system down or worse, plant possible viruses on the system that would en-

able a person to steal or manipulate the income of the property.

GLI will gather all possible known vulnerabilities against a published vulnerabilities database. Scan all ports for possible areas that will help a hacker gain access to the property network.

The Internal Network Risk Assessment will include the following:

- Port scanning of the system and workstations
- Identify vulnerabilities against a published vulnerabilities database
- Identify areas that a potential hacker can gain access

Internal Penetration Assessment: GLI's team will perform an Internal Penetration Assessment. This will enable us to validate the vulnerabilities found during our vulnerability scanning.

The penetration test is a method of evaluating the security of your computer systems and/or network by simulating an attacker. This process involves an active analysis of your system for any weaknesses, flaws or vulnerabilities. The analysis is performed from a potential attacker's position and can involve active exploitation of the security vulnerabilities discovered during the vulnerability scans.

Unlike the vulnerability scans, the penetration testing is mainly a manual process. We will manually probe the target host for common mis-configurations or flaws because a vulnerability scanner can fail to identify certain vulnerabilities.

Wireless Network Risk Assessment Process

This assessment will completely map all wireless access points that are on the property at the time of the assessment. Through this assessment we will be able to identify access points that might be on the network that are not authorized to be there.

GLI will identify the encryption levels and the risks involved in the encryption levels found. We will identify how far the wireless bleeds outside of the property to prevent possible hackers from being outside the property and attempt to hack the system.

The Wireless Network Assessment will include the following:

- Scanning of the wireless system and all access points (APs)
- Identify un-authorized APs on the system, if any
- Identify encryption and let the property know the risks involved in the encryption levels found
- Bleed test to identify the wireless access outside the outlined build
- Identify vulnerabilities against a published vulnerabilities database
- Identify areas that a potential hacker can gain access to

All areas of vulnerabilities that are indentified will follow with an in-depth report to help clear the issues.

Web Application Security Assessment Process

GLI will validate the security of the submitted application. This will enable us to identify possible vulnerabilities or holes in the application that a potential hacker might use to circumvent the intended operation of the application. Our Web application testing methods are used in conjunction with the OWASP methodology. This review will use GLI's Black Box Testing approach. This level of testing will make use of:

- Vulnerability scanning
- Input fuzzing to detect input overruns or failure to validate data
- Network testing to verify data leakage, encryption strength and implementation
- Reverse binary engineering as applicable to determine if in-place changes to the program can alter its functionality

GLI testing includes:

- Information Gathering
- Configuration Management
- Secure Transmission
- Authentication
- Session Management
- Authorization
- Data Validation
- Denial of Service
- Business Logic
- Cryptography
- Risky Functionality - File Uploads
- Risky Functionality - Card Payment
- HTML5