



GLI®

GLI Europe BV

Diakenhuisweg 29-35
2033 AP Haarlem
The Netherlands

Tel +31 (0)88 220 6600
www.gaminglabs.com

Chamber of Commerce
Leiden nr. 28117769
VAT Identification number
NL 8184.73.393.B.01

RvA Registration Number of
Accreditation applicable to this
Report.

Inspection	I111
------------	------

This report is only intended for recipients authorized by GLI. Please visit gaminglabs.com to view the applicable terms and conditions and GLI Product Certification Scheme. If the recipient does not agree to all of such terms and conditions or GLI Product Certification Scheme, GLI withdraws the certification or analysis established by this report and the recipient must immediately return to GLI all copies of this report and make no reference to this report for any purpose at any time.

Worldwide Locations

World Headquarters

Lakewood, New Jersey

International Offices

GLI Africa

GLI Asia

GLI Australia Pty Ltd

GLI Austria GmbH

GLI Europe BV

GLI Italy

GLI South America

U.S. Regional Offices

Colorado

Nevada

Live Studio Audit Report

Prepared for

Evolution Gaming Malta Limited

by:

GLI Europe B.V.
Diakenhuisweg 29-35
2033 AP Haarlem
The Netherlands
Ph: +31 (0)88 220 6600

Report Type:

Audit

File Number:

PS-609-EVM-23-02-246

Jurisdiction:

UK Remote

Document Reference:

Remote Gambling and Software Technical Standards
(February 2021)

Testing Strategy for Compliance with Remote Gambling
and Software Technical Standards February 2021

Report Date:

01 June 2023

Expiration Date:

01 June 2024

*This test report may not be reproduced, other than in full, except with the prior written permission of
GLI Europe B.V.*



TABLE OF CONTENTS

TABLE OF CONTENTS	2
GENERAL INFORMATION.....	3
EVALUATION PROCESS	5
OVERALL EVALUATION	8
EXECUTIVE SUMMARY	9
CONCLUSION	11
CONDITIONS OF EVALUATION	12
AUDITOR'S QUALIFICATION	13
Appendix A. SCORING THE RISKS WITH ISO/IEC 31010:2009 RISK MANAGEMENT - ASSESSMENT TECHNIQUES.....	14

**GENERAL INFORMATION**

Brand

Evolution

PROJECT DETAILS**SCOPE OF WORK****RTS 17**

- a. To ensure that live dealer operations are fair.

RTS requirement 17A

- b. Live dealer operations must be fair and independently auditable.

RTS implementation guidance 17A

- a. Equipment and consumables should be of commercial casino quality. Designated staff should be responsible for monitoring the integrity of all operational equipment.
- b. Croupiers need to undergo adequate training to provide the gambling in a fair way according to documented procedures and game rules. Evidence of training and refresher training should be maintained.
- c. Gambling provision should be supervised by staff responsible to oversee dealer activities and integrity. Video surveillance to record all dealer activity should be in place, enough to cover the predefined gaming areas with sufficient detail to confirm whether dealing procedures and game rules were followed.
- d. Secure areas, gambling equipment and consumables shall be protected by appropriate access controls to ensure that only authorised personnel are allowed access. Game logs should be maintained, and game events collated into statistics which can be analysed for trends relating to game performance, staff and/or locations in the gaming area.
- e. Game logs should be maintained and game events collated into statistics which can be analysed for trends relating to game performance, staff and/or locations in the gaming area.



GENERAL INFORMATION

KEY DATES

Request Date:	03 March 2023
Audit Start Date:	13 March 2023
Audit Completion Date:	23 May 2023



EVALUATION PROCESS

The Live Studio Audit was performed with the intent of identifying any actual or potential instances of non-compliance, vulnerabilities or weaknesses, and assuring that the confidentiality, integrity and availability of the information under Evolution Gaming Malta Limited's control are preserved.

GLI's evaluation approach was based on commonly used security standards and guidelines that provide an industry-accepted foundation developing effective security management practices. This approach relies heavily on layered security in order to reduce the risk to computer and network systems. The layered approach provides redundancy and reinforces the overall security model, as several layers of security must be breached before a critical data store is accessed.

LIVE STUDIO AUDIT

The Live Studio Evaluation includes (but is not necessarily limited to) the following elements:

- Submitted Documentation Review;
- Testing and Evaluations:
 - o Administrative Controls Assessment,
 - o Technical Controls Assessment,
 - o Physical and Environmental Controls Assessment.

The Audit approach is based on the following methods:

- Asking questions (enquiry-based approach)
- Gathering evidence (evidence-based approach)
- Remote assessment and speaking to staff (observation-based approach).

An essential part of GLI's assessment involves reviewing security policy documentation in order to obtain a theoretical understanding of the Information Systems Security and to check for issues of non-compliance with the standards described in the scope of work section.



EVALUATION PROCESS

DOCUMENTATION

Documentation regarding policies, procedures and guidelines on the auditee's processes for information protection was collected by the auditor and reviewed. List of documentation collected and reviewed is retained within GLI systems.

IT SYSTEMS REVIEWED

TESTING TOOLS

No testing tools were used during the audit.

PERSONNEL INTERVIEWED

SUMMARY

The following staff members were interviewed by the audit team:

Name	Role
Michele Bucciano	Operations Manager
Sergejs Likincevs	Physical Security Lead
Marina Lokastova	Operations Manager
Emilian-Viorel Iosif	Equipment Integrity Specialist
Keith Vidolich	Operations Manager
Adam Vall Wallqvist	Operations Manager
Saviour Gauci	Facility Supervisor
Sergejs Bezusconoks	Lead Automation and Controls Systems
Aleksandrs Siskevics	Lead Electrical Engineer
Christabel Psaila	Talent Acquisition Partner

Via Video Conferencing to:

Mriehel – Fort Business Centre, Triq L-Intornjatur, Zone 1, Central, Business District, Birkirkara CBD1050 – Malta (remote)

EVALUATION PROCESS

SUMMARY

The following staff members were interviewed by the audit team (continued):

Name	Role
Claude Falzon Mangion	Studios Senior Compliance Specialist
Jekaterina Melkere	Studios Compliance Specialist
Craig Pickard	Studios Compliance Specialist
Sergejs Likincevs	Physical Security Lead
Anooshavan Isaghoolian	Physical Security Specialist
Arvis Ancupans	Information Security Officer
Mairis Januns	Information System Security Engineer
Karlis Bergmanis	Information Security Specialist
Aleksejs Andasevs	IT Support Department Lead
Aleksandr Mailyan	IT Support Engineer
Carl Muscat	IT Support Engineer
Anna Zilina	Equipment Integrity Manager
Svjatoslavs Berdisevs	Equipment Manager Europe
Tamari Siordia	Customer Support Manager
Medea Shatakishvili	Service Support Manager
Viktorija Jaksina	Customer Support Manager
Marija Kuzjajeva	Service Support Manager
Nils Brunkevics	Risk Analysts Team Lead
Ana Aslanishvili	Risk Analysts Team Lead
Sofja Kotlerova	Risk Analysts Team Lead
Lasha Vekua	Risk Analysts Team Lead
Roberts Auzans	Risk and Integrity System Analyst
Dzintars Vilnis	Research and Development Risk Manager
Ruta Punka	Data Protection Specialist
Guntis Kokins	Operational Excellence Auditor

Via Video Conferencing to:

Mrieħel – Fort Business Centre, Triq L-Intornjatur, Zone 1, Central, Business District, Birkirkara CBD1050 – Malta (remote)



OVERALL EVALUATION

Evolution Gaming Malta Limited is a company that provides live streaming of casino games, with its main operations based in Riga, Latvia. It currently has more than 3000 employees.

The gaming operation and live streaming services forming the scope of this audit is the following live studio location:

- Malta Mriehel – Fort Business Centre, Triq L-Intornjatur, Zone 1, Central, Business District, Birkirkara CBD1050 – Malta

The games offered from this studio include:

- Blackjack
- Roulette
- Top Dice
- Baccarat
- Money Wheel
- Top Card
- Mega Ball
- Hold 'em Poker
- Classic Free Bet Blackjack
- Lightning Roulette
- Speed Baccarat
- Speed Blackjack
- Infinite Blackjack
- Speed roulette

A number of interviews were carried out with company personnel, including specific interviews with the following department/functions:

- Operations Management
- Facilities Management
- Global Physical Security
- Global Information Security
- Global IT Support
- Global Equipment Integrity
- Global Customer Support
- Global Game Integrity & Risk
- Global Operational Quality and Excellence
- Human Resources

PANDEMIC RESTRICTIONS

N/A

EXECUTIVE SUMMARY

Testing Required:

Testing Required/Assurance Activities (Table 1: General risk and compliance assurance activities from the testing strategy document(February 2021))		Determination	Result/Explanation
1	Licensees administering live dealer operations must seek independent assurance their operation conforms to requirements. Assessment to be conducted by a gambling regulator or test house	PASS	

Technical Requirements:

RTS 17			
Gaming (including bingo)			
RTS aim 17		Determination	Result/Explanation
To ensure that live dealer operations are fair.			
RTS requirement 17A		Determination	Result/Explanation
	Live dealer operations must be fair and independently auditable.	PASS	
RTS implementation guidance 17A		Determination	Result/Explanation
a.	Equipment and consumables should be of commercial casino quality. Designated staff should be responsible for monitoring the integrity of all operational equipment.	PASS	
b.	Croupiers need to undergo adequate training to provide the gambling in a fair way according to documented procedures and game rules. Evidence of training and refresher training should be maintained.	PASS	
c.	Gambling provision should be supervised by staff responsible to oversee dealer activities and integrity. Video surveillance to record all dealer activity should be in place, enough to cover the predefined gaming areas with sufficient detail to confirm whether dealing procedures and game rules were followed.	PASS	
d.	Secure areas, gambling equipment and consumables shall be protected by appropriate access controls to ensure that only authorised personnel are allowed access.	PASS	Recommendation: It was noted that although access control to the CCTV surveillance station was in place, the door was being kept open during busy hours. The auditor recommends that the security policy is enforced to ensure that security measures put in place (in this case biometric access control) are not rendered ineffective due to lack of policy enforcement.
e.	Game logs should be maintained and game events collated into statistics which can be analysed for trends relating to game performance, staff and/or locations in the gaming area.	PASS	



PARTIAL AND NON-CONFORMITIES

No partial or non-conformities were identified.



CONCLUSION

Overall, it was found that the level of security achieved in the relevant areas is aligned with the requirements in scope and it is GLI's overall assessment that the auditee (and their management) are moving forward with the full intention to provide a secure, resilient and well managed server environment. There are a number of areas that would benefit from improvement and recommendations have been made to that effect.

Subject to the conditions discussed in this Report, GLI has found that the evaluated elements of the auditee are compliant with the applicable sections of the standard listed herein.

CONDITIONS OF EVALUATION

GLI's Live Studio Audit of the auditee is conditional upon the following:

- The evaluation of the auditee's Live Studio was related to the Information Systems Security only. This excludes any other functions provided by the submission not related to the Information Systems Security or Business Functions.
- The information gathered from auditee's personnel is assumed to be accurate and complete.
- Environmental conditions are assumed to be ideal, and the audit is assumed to be conducted in a full operational environment.
- There are unavoidable limitations inherent to performing a Live Studio Audit within a short period of time, as it is not possible to verify the effects of all of potential configurations and environments that may occur once the site is running in the production for an extended period of time.

Authentication of GLI's Information Systems Security Audit Report of auditee's Live Studio.

Audited by: Jean-Pierre Agius

Reviewed by: Daniel Bonnici

Technical Evaluation authorized by:

A handwritten signature in black ink, appearing to read "M. Britton", written over a light blue horizontal line.

Martin Britton
Managing Director

AUDITOR'S QUALIFICATION

Auditing activity on this project was carried out by:

Jean-Pierre Agius - Author

Experienced information security professional with over seven years of experience in conducting information security and compliance audits. Jean-Pierre's career includes experience as a Systems Auditor with a regulatory gaming authority. Jean-Pierre holds a BSc (Hons.) degree in Business and Information Technology from the University of Malta and also holds the following relevant professional certifications:

- BSc (Hons.) degree in Business and Information Technology
- ISACA Certified Information Systems Auditor (CISA)
- Certified Ethical Hacker (CEH)
- PECB ISO/IEC 27001 Lead Auditor
- PECB ISO/IEC 27001 Lead Implementer
- CompTIA Security+
- CompTIA Secure Infrastructure Specialist (CSIS)
- CompTIA IT Operations Specialist (CIOS)
- CompTIA Network+
- CompTIA A+

GLI Europe BV. has determined that the above auditor has no direct commercial relationships with the audited licensee and attests to the auditor's independence.

APPENDIX A. SCORING THE RISKS WITH ISO/IEC 31010:2009 RISK MANAGEMENT - ASSESSMENT TECHNIQUES

ISO/IEC 31010:2009 Risk Management – Risk assessment techniques is an industry standard for assessing the severity of security threats. It attempts to establish a measure of how much concern a threat warrants, so efforts can be prioritized. The score is based on a series of measurements (called metrics) based on expert assessment.

Base Metrics: for qualities intrinsic to vulnerability. There are six Base Metrics, which represent the most fundamental, immutable qualities of vulnerability.

- Access Vector: measures how remote an attacker can be to attack a target.
- Access Complexity: measures the complexity of attack required to exploit the vulnerability, once an attacker has gained access to the target system.
- Authentication: measures the number of times an attacker must authenticate to the target system in order to exploit the vulnerability.
- Confidentiality Impact: measures the impact on confidentiality of a successful exploit of the vulnerability on the target system.
- Integrity Impact: measures the impact on integrity of a successful exploit of the vulnerability on the target system.
- Availability Impact: measures the impact on availability of a successful exploit of the vulnerability on the target system.

Temporal Metrics: for characteristics that evolve over the lifetime of vulnerability. There are three Temporal Metrics, which represent the time dependent qualities of vulnerability.

- Exploitability: measures how complex the process is to exploit the vulnerability in the target system.
- Remediation Level: measures the level of an available solution.
- Report Confidence: measures the degree of confidence in the existence of the threats and the credibility of its report.

Severity Rankings

Severity	Score	Action Required
 High	Major Non-Conformity	High to Critical threat that needs immediate resolution.
 Medium	Minor Non-Conformity	Moderate risk that needs to be investigated.
 Low	Observation	Issue that needs to be reviewed to ensure good practices.