

CONFIDENTIAL

LGA Compliance Audit Questionnaire

Compliance with the Regulations contained in Legal Notice 176 of 2004 is a requirement for those operators seeking to gain or retain a licence for Remote Gaming in Malta. Compliance with ISO-17799 “Information technology – code of practice for information security management” is desirable for any business reliant on information technology.

This questionnaire is based on the controls of ISO-17799 but is cross-referenced to the particular requirements and regulations of the Remote Gaming regulations extant in Malta.

Some questions may not apply due to the variation between operations and licence classes.

Please give answers which reflect the situation that exists at the time of audit and which can be substantiated with existing documents or data. Supporting evidence will be asked for.

It may help to list all software applications used by the Licensee to perform remote gaming from Malta and assign them short names for use in filling details relating to the questionnaire.

| Outline of remote gaming application | Short name used below | Class of LGA Licence |
|---|------------------------------|-----------------------------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Add continuation sheets if necessary.

Throughout the questionnaire (pages 4-30) below, the Gaming System(s) are referred to in the plural in recognition that one Licensee may be running multiple gaming applications on his server or servers. If the answers for different applications vary, please use the Comment space to reference extra notes on continuation sheets as required.

The Control System is referred to as a singular item even though it may be made up of multiple software applications (betting risk management software, accounts, payment processing routines and other utilities) which are expected to function together and report directly to the Key Official. The records generated by the Control System must be in Malta.

DEFINITION – “user” is a person employed by or acting for the licensee; a “player” accesses the licensee’s gaming system(s) in order to tender a bet.

Please refer to the LN176 Remote Gaming regulations for other definitions – the regulations are available as a PDF file on request. This questionnaire is also available as a PDF file, but remains the copyright of LGA and may not be disclosed to any unauthorized third party.

CONFIDENTIAL

ISO -17799 Information Technology – Code of practice for information security management controls as adapted for LGA

1. Control System

- 1.1 Establish the Control System (PLAN)
- 1.2 Implement and Operate the Control System (DO)
- 1.3 Monitor and review the Control System (CHECK)
- 1.4 Maintain and improve the Control System (ACT)
- 1.5 Management responsibility - including anti-money laundering procedures, Player Protection

2. Documentation requirements

- 2.1 General – including financial reporting aspects
- 2.2 Control of documents – to reference operating from Malta
- 2.3 Control of records – to be available/kept in Malta

3. Security Policy

- 3.1 Information Security Policy; Key Official responsibilities

4. Organisational Security

- 4.1 Information Security Infrastructure
- 4.2 Security of Third Party Access
- 4.3 Outsourcing

5. Asset Classification and Control

- 5.1 Accountability for assets
- 5.2 Information classification

6. Personnel Security

- 6.1 Security in job definition and resourcing
- 6.2 User training
- 6.3 Responding to security incidents and malfunctions

7. Physical and environmental security

- 7.1 Secure areas
- 7.2 Equipment security
- 7.3 General controls

8. Communications and Operations Management

- 8.1 Operational procedures and responsibilities
- 8.2 System planning and acceptance
- 8.3 Protection against malicious software
- 8.4 Housekeeping
- 8.5 Network management
- 8.6 Media handling and security; mirroring
- 8.7 Exchanges of software and information

9. Access control

- 9.1 Business requirement for access control
- 9.2 User access management
- 9.3 User responsibilities
- 9.4 Network access control
- 9.5 Operating system access control
- 9.6 Application system access control
- 9.7 Monitoring system access and use
- 9.8 Mobile computing and teleworking

10. Systems Development and Maintenance

- 10.1 Security requirements of systems
- 10.2 Security in application systems
- 10.3 Cryptographic controls
- 10.4 Security of system files
- 10.5 Security in development and support processes

11. Business continuity management

- 11.1 Aspects of business continuity management
- 11.2 Liabilities related to DRP – legal and financial

12. Compliance

- 12.1 Compliance with legal requirements
- 12.2 Review of security policy and technical compliance
- 12.3 System audit considerations

| 1.1 | Establish the Control System (PLAN) | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 1.1.1 | Has the Control System been completely documented in accordance with regulation 20? | | | |
| | Are all the Gaming System(s) in use subject to this documented Control System? | | | |
| | Are the Control System procedures and records held in Malta at this point in time as per regulation 50? | | | |
| | Has the Control System been approved by the owners of the licensed operation based in Malta? | | | |
| | Is the Control System managed by the Key Official in accordance with regulation 15? | | | |
| | Is the Key Official registered as resident in Malta? | | | |
| 1.1.2 | Is there a formal approach to Game Risk Management in the Control System? | | | |
| | Is there a formal approach to IT/Communications Risk Management in the Control System? | | | |
| 1.1.3 | Are there any written policies for risk management? | | | |
| | Are there any procedures for reporting risks? | | | |
| 1.1.4 | Has the licensee included the value of their Gaming software and/or the data in their Balance Sheet? | | | |
| | Has the licensee computed the cost of past or future security breaches? | | | |
| | Has the licensee any means of costing risks? | | | |
| 1.1.5 | Is it clear who is responsible for addressing risks to the Gaming System(s) and in the Control System? | | | |
| 1.1.6 | Are there policies for avoiding risks e.g. fraud screen; players blacklist database? | | | |
| | Does the licensee have protection relating to perceived risks e.g. insurance, bonds, guarantees? | | | |
| 1.1.7 | Does the Control System satisfy all the requirements of regulation 20(2) of LN176? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 1.2 | Implement & Operate the Control System (DO) | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 1.2.1 | Are there staff resources assigned to setting up and maintaining the Control System? | | | |
| | Is all remote gaming conducted under the Control System as per regulation 24? | | | |
| | Is there a budget for training staff on info security? | | | |
| | Does the licensee employ any Third Party to check their systems or advise on security precautions? | | | |
| | Are there staff resources assigned to setting up and maintaining the Game Risk Management System? | | | |
| 1.2.2 | Does the Control System address (in some fashion – may be avoid, reduce, transfer or accept) all the risks considered relevant to the Gaming System(s)? | | | |

| 1.3 | Monitor & review the Control System (CHECK) | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 1.3.1 | Does the Control System include monitoring procedures to detect vulnerabilities? | | | |
| 1.3.2 | Are there procedures in place to eliminate or mitigate gaps in the Control System? | | | |
| 1.3.3 | Is there a systematic method to improve the Control System and the Gaming System(s) it manages? | | | |

| 1.4 | Maintain & improve the Control System (ACT) | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 1.4.1 | Are improvements to the Control System made? | | | |
| 1.4.2 | Are recurring problems encountered due to gaps or excesses in the Control System? | | | |
| 1.4.3 | Is the Control System pro-active in anticipating threats to the licensee based on industry news? | | | |
| | Does the Licensee have a Game Risk manager? | | | |
| | Does the Licensee have an IT Risk manager? | | | |
| | Are significant changes to the Control System notified to the LGA as per regulation 20 last clause? | | | |

| 1.5 | Management responsibility (including AMOL, Player Protection) | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 1.5.1 | Is there commitment to the Control System at all stages of the management chain? | | | |
| | Are Anti Money Laundering measures in place? | | | |
| | Are Player Protection measures in place? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 2.1 | Documentation Requirements | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| | Does the Control System define the records kept in accordance with regulation 50? | | | |
| | Does the Control System provide a true and fair view of financial position via its accounting records in accordance with regulation 51? | | | |
| | Does the Control System include filing of financial statements in accordance with regulation 52? | | | |
| 2.1.1 | Does licensee reserve funds sufficient to cover player deposits at any point in time? | | | |
| | Does licensee maintain separate accounts for players' funds (deposited but not committed to bets)? | | | |
| | Does licensee generate monthly Management Accounts? | | | |
| 2.1.2 | Is there a clear process for authorising documents before they are released to LGA, MFSA or others? | | | |
| | Is there a process to review and update operating procedure documents as necessary? | | | |
| | Are internal documents subject to version control? | | | |
| | Are all Control System/operating procedure documents available for inspection in Malta? | | | |
| 2.3.1 | Are there records to show that the Control System has been applied to daily operations? For example, are updates to the software signed off and filed? | | | |
| | Are all bank statements related to the Gaming System(s) or Control System(s) available in Malta? | | | |
| | Are all accounting systems related to the Gaming System(s) or Control System(s) available in Malta? | | | |
| | Are Gaming System(s) audit trails and other monitoring procedures available in Malta? | | | |
| | Are audit trails archived in Malta? | | | |
| | Are the archives maintained in a fashion which would render their content legally admissible? | | | |
| | Is access to the records above limited to staff and LGA representatives? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 3.1 | Information Security Policy Document (ISP) | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 3.1.1 | Is there an Information Security Policy (ISP) document? | | | |
| | Are staff aware of the ISP document content? | | | |
| 3.1.2 | Is there a person responsible for writing and applying the ISP for the licensee? | | | |
| | Is there a log of incidents reported? | | | |
| | Are the costs and benefits of the ISP reviewed? | | | |
| | How often is the content of the ISP reviewed? | | | |
| | Has a copy of the ISP been provided to LGA? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 4.1 | Information Security Infrastructure | Yes | No | Comment |
|-----|--|-----|----|---------|
| | Is the Key Official responsible for security aspects of the Gaming and Control systems? See regulation 15(2)(a). | | | |
| | Are changes to the Gaming or Control Systems under the control of the Key Official? | | | |
| | Does the Key Official know who to contact at LGA or other relevant law enforcement agency in the case of a security breach requiring follow-up action? | | | |

| 4.2 | Security of Third Party Access | Yes | No | Comment |
|-----|--|-----|----|---------|
| | Does the licensee permit Third Party Access to its Gaming or Control Systems? [Explanation = Are persons not on the payroll of the licensee given user (not player) accounts on the gaming or financial systems such as allow them to create, read, update or delete privileged information in those systems?] | | | |
| | Does the licensee ask if such Third Party trading partners are ISO-17799 compliant? | | | |

| 4.3 | Outsourcing (the assigning of non-core activities to Third Parties) | Yes | No | Comment |
|-----|---|-----|----|---------|
| | Is Operating System maintenance outsourced? | | | |
| | Is Networking System maintenance outsourced? | | | |
| | Are Payment Systems programming outsourced? | | | |
| | Is Gaming System programming outsourced? | | | |
| | Are software testing functions outsourced? | | | |
| | Are accounting functions outsourced? | | | |
| | Are payroll functions outsourced? | | | |
| | Are call centre functions outsourced? | | | |
| | Are data entry functions outsourced? | | | |
| | Are any other functions outsourced? | | | |
| | Does the licensee ask if the outsourced trading partners are ISO-17799 compliant? | | | |

Wherever there are functions outsourced which can affect the result of the remote gaming system, or the related financial systems, the contract governing this arrangement must be provided to LGA.

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 5.1 | Accountability for assets | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| | Is regulation 36 satisfied by the Control System procedures? (Payment to players) | | | |
| | Is regulation 37 satisfied by the Control System procedures? (Remission of funds) | | | |
| | Is regulation 38 satisfied by the Control System procedures? (Dealing with players' monies restricted) | | | |
| | Is regulation 40 satisfied? (Clients funds are to be held in separate accounts from the licensees funds) | | | |
| | Is regulation 41 satisfied? (Licensee authorizes the bank holding clients funds to disclose information to LGA on request) | | | |
| | Will the licensee mark the financial reports sent to LGA under regulation 52 as "Confidential"? | | | |
| | Does the licensee assign a financial value to its database of players or its gaming systems? | | | |
| | Does the licensee assign financial value to its database of agents/resellers - if relevant? | | | |
| | Are there aspects of the gaming system for which there may be Intellectual Property Rights value? | | | |
| | Is the licensee obliged to protect the source code of the gaming system (where it is leased for example)? | | | |

| 5.2 | Information classification | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| | Does the Control System assign particular ownership and control for sensitive information? | | | |
| | Is there a single registry for Control System files (electronic or manual) held by the licensee? | | | |
| | Is the "need to know" principle applied to data sharing, email and document circulation? | | | |
| | Is there a system to review/purge/archive data? | | | |
| | Is there a system to re-validate data? | | | |
| | Is data mining practiced on live data for any reason? | | | |
| | Are all active players registered in accordance with regulations 32 and 35 which require both betting accounts and financial accounts to be maintained per player, kept congruent and secure? | | | |
| | Do all Gaming System(s) used satisfy the information requirements of the Third Schedule to LN176? (Audit trails are to be kept and archived). | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 6.1 | Security in job definition and resourcing | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| | Do generic security duties show in employment contracts? [like controlling computer viruses] | | | |
| | Are specific security duties included in employment contracts? [like managing a Firewall] | | | |
| | Are all staff engaged in the Gaming or Control systems referred to LGA as part of the vetting process BEFORE being engaged? | | | |
| | Are contract staff or consultants ever employed? | | | |
| | If contract staff/consultants are employed, are they vetted before being allowed access to the Gaming or Control system? | | | |
| | Do all staff working on the Gaming or Control System sign a Confidentiality Agreement? | | | |
| | Do all contractors, consultants or other Third Parties with access to the Gaming or Control System sign a Confidentiality Agreement with the licensee? | | | |

| 6.2 | User training | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| | Are all staff made aware of the type of security threats relevant to their work (for example, email and internet infections, risks of viruses if connecting flash memory or PDAs onto the office systems)? | | | |
| | Is awareness of the ISP (if it exists) checked amongst the Gaming and Control system staff? | | | |
| | Are staff informed how, and rewarded for, escalating security incidents, perceived weaknesses or evident malfunctions in the Gaming or Control systems? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 6.3 | Responding to Security Incidents and Malfunctions (Licensee's own operations) | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 6.3.1 | Is it clear what constitutes a security incident affecting the Gaming system(s)? [Proposed explanation – any abuse or exploitation which attempts to distort the result of a game or alter the payout should be considered a security incident; unfocussed, weak attacks on firewalls need not be treated as individual security incidents if they are effectively blocked by the existing precautions.] | | | |
| | Is it clear what constitutes a security incident affecting the Control system? [Proposed explanation – any abuse or exploitation which attempts to distort the financial results or payments should be considered a security incident; unfocussed, weak attacks on firewalls need not be treated as individual security incidents if they are effectively blocked by the existing precautions.] | | | |
| | Are staff aware of how and when to escalate a report concerning a security incident? | | | |
| 6.3.2 | Are staff aware of how and when to escalate a report concerning a security weakness? | | | |
| 6.3.3 | Are staff aware of how and when to escalate a report concerning a security malfunction? | | | |
| 6.3.4 | Is the Key Official in a position to review all security incidents, weaknesses and malfunctions? | | | |
| | Is there any analysis done to identify common causes of security incidents, weaknesses or malfunctions? | | | |
| | Is there any analysis done to identify the costs of security incidents, weaknesses or malfunctions? | | | |
| | Is this review process fed back into the next ISP? | | | |

Many security incidents originate internally and must be screened for/logged.

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 7.1 | Secure Areas | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 7.1.1 | Are the offices where the Gaming System(s) is/are managed physically segregated from other activities and public areas so that access is restricted to staff? | | | |
| | Are the offices where the Control System is managed physically segregated from other activities and public areas so that access is restricted to staff? | | | |
| | Can the official routes of access be bypassed through roof voids, floor spaces or other offices? | | | |
| | Are security personnel employed at the entrance? | | | |
| 7.1.2 | Do the offices where the Gaming System(s) is/are managed have programmable access control devices such as swipe cards or code pads? | | | |
| | Do the offices where the Control System is managed have programmable access control devices such as swipe cards or code pads? | | | |
| | Are changes to the cards or codes made by the licensee? (Maybe under control of landlord) | | | |
| | Are the cards or codes changed often? | | | |
| | Is there a key safe for traditional keys? | | | |
| | Is there a fire safe for important documents and/or backup media? | | | |
| | Are there off-site backup facilities? | | | |
| | Are there off-line backup facilities? | | | |
| 7.1.3 | Are servers and telecommunications equipment used by the gaming system protected from environmental hazards (lightning or power surges, flooding, overheating)? | | | |
| | Are servers and telecommunications equipment used by the gaming system protected from unauthorised access or damage? | | | |
| | Are there automated systems to protect the servers and telecommunications equipment: <ul style="list-style-type: none"> • CCTV • Smoke • Heat • Fire • Movement • Humidity | | | |
| 7.1.4 | Are unoccupied offices with sensitive equipment or information kept locked? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 7.2 | Equipment Security | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 7.2.1 | Is sensitive office equipment sited to avoid interference or being overlooked? | | | |
| | Are laptops used to store sensitive and/or vital information? If so, detail backup procedures. | | | |
| | Are Wireless connections employed in the office? | | | |
| | Are Wireless networks protected by protocols such as WEP, WPA, VPN? | | | |
| | Is a shredder available for sensitive waste paper? | | | |
| 7.2.2 | Are surge protectors provided on mains and telecommunications supply? | | | |
| | Are UPSs available to support the core Gaming System servers and terminals? | | | |
| | Are UPSs available to support the Gaming System printers, email, PABX and fax machines? | | | |
| | Are UPSs available to support the core Control System servers and terminals? | | | |
| | Are UPSs available to support the Control System printers, email, PABXs and fax machines? | | | |
| | Is a UPS available to provide emergency lighting? | | | |
| | Are all UPSs tested regularly? | | | |
| 7.2.3 | Is cabling run through ducts or false floors? | | | |
| | Are cabling junctions or patch panels kept secured? | | | |
| 7.2.4 | Is equipment maintained only by suitably trained and authorised personnel? | | | |
| | Are equipment maintenance records and fault reports kept to provide management information? | | | |
| | Are software and hardware configuration records kept to allow for planned maintenance? | | | |
| | Are hard disks removed from hardware which is to be sent offsite for repair? | | | |
| 7.2.5 | Are staff who are authorised to take office equipment offsite (especially laptops) aware of the duty of care involved? | | | |
| | Is the transfer of sensitive data between office equipment and home equipment prohibited? | | | |
| | Are all laptops taken off-site password protected? | | | |
| 7.2.6 | Are there procedures for equipment disposal? | | | |
| | Are electronic media systematically destroyed if no longer required or reliable? | | | |
| | Is an inventory of equipment maintained? | | | |
| | Is an inventory of media in use maintained? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 7.3 | General Controls | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 7.3.1 | Is there a clear desk policy in operation? [This means that all papers are filed whenever the person leaves their desk for an extended period such as overnight] | | | |
| | Is there a clear screen policy in operation? [This involves setting up a screen saver that hides the user's activities after a time-out period; it should require a password to be de-activated] | | | |
| | Are there lockable cabinets or offices for sensitive files? | | | |
| 7.3.2 | Is authorisation for removal of any asset (hardware, software or data) required prior to its leaving the licensee's offices? | | | |
| | Are laptops assigned to specific users? | | | |
| | Are PDAs used by staff? | | | |
| | Are all emails and attachments screened for malicious code? | | | |
| | Is regulation 26(2)(g) satisfied for all Gaming System(s) in use in respect of physical and environmental security? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 8.1 | Operational Procedures & Responsibilities | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| | Is regulation 26 satisfied for all Gaming System(s) in use? Communications and operational data must be maintained current at all times and available in Malta for inspection by LGA. | | | |
| | Is regulation 27 satisfied for all Gaming System(s) in use? No significant changes to live operations are allowed without prior approval of LGA. | | | |
| 8.1.1 | Are the Gaming System(s) procedures, responsibilities and configurations documented? | | | |
| | Are the Control System procedures, responsibilities and configurations documented? | | | |
| | Do all procedure documents show author/version? | | | |
| | Are backup systems/fallbacks documented? | | | |
| | Are there procedures for the control of portable media such as floppy disks, CDs, tapes, flash memory or removable hard disk drives? | | | |
| | Are procedures stored or available offsite by means of intranet or backup copies? | | | |
| 8.1.2 | Is there a formal change control methodology for all Gaming System(s)? | | | |
| | Is the Key Official involved in Change Control approval and management? | | | |
| | What Third Parties have access to the Change Control records apart from staff of the licensee? | | | |
| 8.1.3 | Does the incident management procedure include reporting up the management chain? | | | |
| | Are all staff aware of the incident reporting process? | | | |
| 8.1.4 | Is there a clear separation between staff engaged in the Gaming System(s) from those engaged in the Control System? | | | |
| | Does the Key Official have maximum privileges on the Gaming System(s)? | | | |
| | Does the Key Official have maximum privileges on the Control (Accounting) Systems? | | | |
| | Do large payments (as defined in Regulation 36) require validation? | | | |
| | Does the licensee have Fraud Prevention measures in place? | | | |
| 8.1.5 | Are there procedures for the design, development and testing of changes to the Gaming System(s)? | | | |
| | Is any software design done by staff of the licensee? | | | |
| | Is any development done by staff of the licensee? | | | |
| | Is any software testing done by staff of the licensee? | | | |
| | Is the website maintained by staff of the licensee? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by

on

| 8.2 | System Planning & Acceptance | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 8.2.1 | Is there a regular assessment of the projected growth of the Gaming System(s) and its processing requirements? There may be need to add servers, routers and bandwidth as business expands. | | | |
| | Is there regular communication with the hosting provider(s) to confirm their ability to handle increased traffic? | | | |
| | Are statistics kept on traffic and peak loading? | | | |
| | Is the office power supply and UPS provision reviewed as staff are added? | | | |
| 8.2.2 | Is there a formal acceptance process when new gaming system functions or features are added? | | | |
| | Does acceptance of new software include testing its security features? | | | |
| | Does acceptance of new software include testing its fit with existing contingency plans and backups? | | | |
| | Does acceptance of new software include requiring training for appropriate staff and management? | | | |

| 8.3 | Protection against Malicious Software | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 8.3.1 | Do staff know that they are responsible for avoiding the introduction of malicious software from uncontrolled media or websites? This precaution may be detailed in the ISP or in an “Acceptable Use Policy” document signed by staff. | | | |
| | Are staff aware that they are responsible for containing any spread of malicious software (by warning those who may have been infected)? | | | |
| | Do staff know what to do if they suspect that malicious software has gained access to the Gaming or Control systems? | | | |
| | Is virus scanning software installed on all office computers? | | | |
| | Are there systems in place to update the virus scanning software of all office computers? | | | |
| | Are there appropriate firewalls in place to protect the office systems? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 8.4 | Housekeeping | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 8.4.1 | Are back-up copies of data and software held by the Licensee in Malta? | | | |
| | Are back-up copies of data and software held in Malta kept in a separate location? | | | |
| | Are back-up copies of data and software held by the Licensee outside Malta? | | | |
| | Is the Restoration of operations from these Backups tested regularly? | | | |
| | Is the Restoration of operations from these Backups tested after each significant software upgrade? | | | |
| 8.4.2 | Are machine generated/automatic audit trails turned on within the Gaming System(s) and underlying databases? | | | |
| | Are these audit trails reviewed by Licensee staff? | | | |
| | Are these audit trails archived? Detail. | | | |
| 8.4.3 | Is there a single depository for any fault found in the Gaming System(s)? | | | |
| | Are these fault logs reviewed by Licensee staff? | | | |
| | Are these faults escalated with an external Third Party for resolution? | | | |
| | Are complaints or comments from Players using the Gaming System(s) also recorded in this fault logging system? | | | |

| 8.5 | Network Management | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 8.5.1 | Are there controls in place to protect data exchanged over the office LAN and the external network connections used by the Licensee? | | | |
| | Do these controls include Firewalls – if so, who configures and maintains them? | | | |
| | Do these controls include Gateways – if so, who configures and maintains them? | | | |
| | Does the office use Wireless devices and routers – if so, who configures and maintains them? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 8.6 | Media Handling & Security | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 8.6.1 | Are there practical rules governing the movement of removable computer media from the office environment where the Gaming System(s) run? | | | |
| | Do the procedures governing movement of such media prevent unauthorised copying, damage or corruption? | | | |
| | Are there equivalent rules to control the transmission of gaming data by other means? (email, mobile or internet transmission) | | | |
| 8.6.2 | Where archives are purged or media is no longer required/no longer reliable, are there procedures governing its disposal? | | | |
| | If the media contains confidential data, will it be marked to indicate this without requiring to be read? | | | |
| 8.6.3 | Are staff aware of the significance of markings such as “Confidential” and how this impacts the handling and disclosure of that information? | | | |
| 8.6.4 | How is the Gaming System(s) documentation protected from entering the public domain? | | | |
| | Has the risk of disclosure of the Gaming System(s) documentation been assessed? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 8.7 | Exchanges of Information & Software with other Third Parties; not play via Gaming System | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 8.7.1 | Where data or software is routinely exchanged, are there appropriate agreements defining the liabilities? [For example if data is imported from a Third Party and later found to be corrupt, whose liability would any losses resulting be?] | | | |
| | When data or software is exchanged, is it triggered by the other party? | | | |
| | When data or software is exchanged, is it validated? | | | |
| | When data or software is exchanged, is a receipt routinely given? | | | |
| 8.7.2 | Where media or data is routinely exchanged between known parties such as Payment Gateways, are there agreements and procedures in place? | | | |
| | Where media or data is routinely exchanged with unknown parties (such as Players), are there rules in place to define the liabilities? | | | |
| | Where media or data is routinely exchanged with unknown parties (such as Players), are there procedures in place to prevent misuse or corruption? | | | |
| 8.7.3 | Is encryption used in the Gaming System on login? [Are users routed through an HTTPS connection?] | | | |
| | Are the Gaming System(s) database(s) encrypted? | | | |
| | Is a full archive of play kept in order to establish “non-repudiation” of the transaction? | | | |
| | Are Player transaction records kept indefinitely? | | | |
| | Are online sessions managed in such a way that a failure of the communications link would allow either resumption of play or refund of stake? | | | |
| | Are all digital certificates relating to the Gaming System(s) current? | | | |
| | Is the renewal date of digital certificates relating to the Gaming System(s) part of the Control System? | | | |
| | Are credit cards deposits accepted in Gaming System(s)? | | | |
| | Are credit cards numbers stored within the Gaming or Control System? | | | |
| 8.7.4 | Is Customer Care conducted via e-mail? If so, what is the relevant address? | | | |
| | Are any Player payment details passed via e-mail? | | | |
| | Are any Player password details passed via e-mail? | | | |
| | Is Gaming software/data ever exchanged via e-mail? | | | |
| | Is encryption used on any e-mail related to the Gaming System(s) or Control System? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by

on

| | | | | |
|-------|---|--|--|--|
| | Is all e-mail passed through a spam filter? | | | |
| | Is all e-mail that is automatically quarantined or rejected reviewed? | | | |
| | Are there procedures to “blacklist” or “whitelist” specific sources of e-mail? | | | |
| | Is Internet Chat used in addition to e-mail? | | | |
| 8.7.5 | Is there an “Acceptable Use Policy” for staff relating to use of office systems including internet and e-mail? | | | |
| | Are staff aware of their obligations under this? | | | |
| | Are staff aware that their use of office systems may be monitored? | | | |
| 8.7.6 | Remote Gaming System(s) being publicly available over the internet are very prone to hacking or Denial Of Service (DOS) type attack. Are controls in place to alert management of any serious attempt to change the information contained in the Gaming System or to overwhelm it with false traffic? | | | |
| 8.7.7 | Are there any controls on the use of the following: <ul style="list-style-type: none"> • Mobile phones • Hands free phones • Internet chat By staff working with the Gaming System? | | | |
| | Are staff restrained from working with competitors? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 9.1 | Business Requirement for Access Control | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| | Are regulations 26 and 27 satisfied for all Gaming System(s) in use? User access control information must be maintained current and available in Malta. | | | |
| | Is regulations 32 satisfied for all Gaming System(s) in use? Registered player information must be maintained current and available in Malta. | | | |
| 9.1.1 | Is there an Access Control Policy in use for staff? [Are staff grouped into to categories whereby their access is set according to their job? Such routines are often built into the Gaming System(s) software.] | | | |
| | Does the Key Official set staff access rights? | | | |
| | Is there an Access Control Policy in use for Players? [Are Players grouped into to categories whereby their games are varied according to their history or value? Such routines maybe built into the Gaming System(s) software.] | | | |
| | Does the Key Official set Player access rights? | | | |
| | Does the Gaming System default to limited access rights for a new Player account? | | | |

| 9.2 | User Access Management | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 9.2.1 | Is there any offline record of the creation, update or deletion of staff accounts on the Gaming System? | | | |
| 9.2.2 | Are accurate and complete records maintained of the access privileges on all Gaming System(s) and all parts of the Control System (accounts, etc)? | | | |
| 9.2.3 | Are staff contractually accountable for the security and use of their passwords? | | | |
| | Are Players contractually accountable for the security and use of their passwords? | | | |
| 9.2.4 | Is there any regular review done to clear away redundant staff accounts on the Gaming System(s)? | | | |
| | Is there any regular review done to validate the access privileges granted to staff ? | | | |
| | Is it policy to disable a staff account as soon as the person ceases employment? | | | |
| | Is there any regular review done to clear away defunct Player accounts on the Gaming System(s)? | | | |
| | Is there any regular process to clear away duplicate Player accounts on the Gaming System(s)? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by

on

| 9.3 | User Responsibilities | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 9.3.1 | Are users given advice on how to choose a strong password which is not easily guessed nor forgotten? | | | |
| | Are Players given advice on how to choose a strong password which is not easily guessed nor forgotten? | | | |
| 9.3.2 | Are staff who have access to the Gaming System(s) or Control System advised not to leave their terminals logged on when unattended? | | | |
| | Are staff who have access to the Gaming System(s) or Control System who leave their terminals logged on unattended disciplined/held liable? | | | |

| 9.4 | Network Access Control | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 9.4.1 | Are staff assigned network access rights according to the job? | | | |
| | Do staff see only the directories and files for which they have access rights? | | | |
| | Do Players see only the games and features for which they have access rights? | | | |
| 9.4.2 | Are “Enforced Paths” used for connections carrying sensitive information - such as between agents and the Gaming System(s) server? | | | |
| | Do all staff have full internet access? | | | |
| 9.4.3 | Is all remote user access to the Gaming System(s) or Control System authenticated? Detail. | | | |
| 9.4.4 | Is all remote computer node access to the Gaming System(s) or Control System authenticated? Detail. | | | |
| 9.4.5 | If diagnostic ports exist in the Gaming System(s) or Control System servers, have suitable controls been put in place to manage their use and prevent abuse? | | | |
| 9.4.6 | Has any risk analysis been done to assess whether there should be logical segregation of traffic (with the need to add Gateways and/or Firewalls) between the Remote Gaming System(s) and/or the Control System? | | | |
| 9.4.7 | Are there any network connection controls to limit traffic according to: <ul style="list-style-type: none"> • e-mail only - according to user type • one-way transfer - according to connection • restriction - according to time of day | | | |
| 9.4.8 | Are there any routing controls built into the Gaming System(s) or Control System network? | | | |
| 9.4.9 | Is it clear who is responsible for the Gaming System(s) networking security? | | | |
| | Is it clear who is responsible for the Control System | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| | | | | |
|--|--|--|--|--|
| | networking security? | | | |
| | Has any risk analysis been done on the risk to traffic passing to and from the Gaming System(s)? | | | |
| | Has any vulnerability tests been done for traffic passing to and from the Gaming System(s)? | | | |
| | Has any risk analysis been done on the risk to traffic passing to and from the Control System? | | | |
| | Has any vulnerability tests been done for traffic passing to and from the Control System? | | | |
| | Is complete and accurate documentation maintained for the physical and logical network relevant to the Gaming System(s)? | | | |
| | Is complete and accurate documentation maintained for the physical and logical network relevant to the Control System? | | | |
| | Does such network documentation include details of the hardware and software security controls in use? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 9.5 | Operating System Access Control | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 9.5.1 | Has any risk analysis been done on limiting access to sensitive parts of the Control System to specified terminals only (which are securely located)? | | | |
| 9.5.2 | Are there any automatic reports generated by multiple login attempts? | | | |
| | Are multiple login failures treated as suspicious? | | | |
| 9.5.3 | Are there Group Login accounts for staff working on the Remote Gaming System(s)? | | | |
| | Are there Group Login accounts for staff working on the Control System? | | | |
| | Do staff accounts become de-activated after a set period of inactivity? | | | |
| | Is Player activity on the Remote Gaming System(s) always traceable to an individual? | | | |
| | Do Player accounts become de-activated after a set period of inactivity? | | | |
| | Can a Player log in more than once simultaneously? | | | |
| 9.5.4 | Is there a password management system in use? | | | |
| 9.5.5 | Are system utilities sometimes used to amend the Gaming System(s) data or Control System records [to correct corrupt data or re-index for example] | | | |
| | Are records kept of every time a system utility is used which bypasses the normal application controls and audit trails? | | | |
| 9.5.6 | Has a risk assessment been made of any staff who may be put under duress? If there is a risk of this, have countermeasures or alarms been implemented? | | | |
| 9.5.7 | Do terminal logins time-out after inactivity? | | | |
| 9.5.8 | Do online sessions time-out after inactivity? | | | |

| 9.6 | Application Access Control | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| 9.6.1 | Do the Gaming System(s) provide logical access controls for staff according to their job? | | | |
| | Do the Gaming System(s) provide logical access controls for Players according to their profile? | | | |
| | Does the Control System provide logical access controls for staff according to their job? | | | |
| 9.6.2 | Has a risk analysis been done to assess if the Gaming System(s) should have an isolated environment? | | | |
| | Has a risk analysis been done to assess if the Control System should have an isolated environment? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 9.7 | Monitoring System Access & Use | Yes | No | Comment |
|------------|--|------------|-----------|----------------|
| | Do all Gaming System(s) satisfy regulation 47 governing recovery from aborted game? | | | |
| | Do all Gaming System(s) satisfy regulation 48 governing recovery from a miscarried game? | | | |
| 9.7.1 | Are all events within the Gaming System(s) logged? | | | |
| | Are all events within the Control System logged? | | | |
| | Are all users aware that events are logged? | | | |
| 9.7.2 | Have a set of events which are to be monitored be drawn up by management? | | | |
| | Are the set of events which are monitored checked on a regular basis? | | | |
| | Are the events which are monitored checked by some-one who is independent of those events? | | | |
| | Are the events which are monitored checked by some-one who is sufficiently experienced? | | | |
| 9.7.3 | Are all Gaming System(s) server clocks synchronised with a respected source? | | | |

| 9.8 | Mobile Computing & Teleworking | Yes | No | Comment |
|------------|---|------------|-----------|----------------|
| 9.8.1 | Has any risk analysis been done on the use of laptops by senior staff or their remote access to the Gaming System(s)? | | | |
| | Has any risk analysis been done on the use of laptops by senior staff or their remote access to the Control System? | | | |
| | Is the storage of core data onto laptops considered part of the Licensee's Disaster Recovery Plan? | | | |
| 9.8.2 | Do any staff involved in the Gaming System(s) regularly work from home? | | | |
| | Do any staff involved in the Control System regularly work from home? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 10.1 | Security Requirements of Systems | Yes | No | Comment |
|-------------|---|------------|-----------|----------------|
| 10.1.1 | Are security measures included at the design stage? | | | |
| | Are system changes made in a controlled fashion? | | | |
| | Do all Gaming System(s) satisfy the technical requirements of regulation 25 (Third Schedule) requiring game result to be independent of the gaming device or communications link? | | | |
| | Are system changes designed to meet compliance objectives? | | | |

| 10.2 | Security in Application Systems | Yes | No | Comment |
|-------------|--|------------|-----------|----------------|
| | Do all Gaming Systems in use satisfy regulations 25, 26 and 27 in respect of their security features? See also the technical specifications in the Third Schedule relating to regulation 25. | | | |
| 10.2.1 | Do staff enter data manually on behalf of customers/Players? [Telephone bets for example] | | | |
| | Is data entry by staff validated before? | | | |
| | Is data entry by staff checked afterwards? | | | |
| 10.2.2 | Has risk analysis been done on the Gaming System(s) internal processes to assess what checks may be appropriate to ensure data integrity? | | | |
| | Are there regular validation checks run on the Gaming System(s)? | | | |
| 10.2.3 | Is message authentication considered relevant to traffic with Gaming System(s) or Control System? | | | |
| 10.2.4 | Are there output/payment checks applied to the Gaming System(s) or Control Systems? | | | |
| | Are the staff who run output/payment checks independent of those who input data? | | | |

| 10.3 | Cryptographic Controls | Yes | No | Comment |
|-------------|---|------------|-----------|----------------|
| 10.3.1 | Do the Gaming System(s) require a random number generator to arrive at the game result? | | | |
| 10.3.2 | Is encryption used for external traffic concerning the Gaming System(s)? | | | |
| | Is encryption used internally for data held in the Gaming System(s)? | | | |
| 10.3.3 | Are digital signatures routinely used in the Gaming System(s)? | | | |
| 10.3.4 | Is encryption data retained to prove receipt and dispatch of Gaming System(s) transactions? | | | |
| 10.3.5 | Is there a person appointed as responsible for cryptographic key management? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 10.4 | Security of System Files | Yes | No | Comment |
|-------------|--|------------|-----------|----------------|
| 10.4.1 | Is there a version control system in place for all live Gaming System(s)? | | | |
| | Are old versions of the Gaming System(s) archived? | | | |
| | Can Gaming System(s) upgrades be rolled back? | | | |
| 10.4.2 | Is Live data used to construct test data? | | | |
| | When Live data is copied for test purposes, is it sanitized to avoid privacy issues? | | | |
| 10.4.3 | Does the Licensee have access to the source code of the Gaming System(s)? | | | |

| 10.5 | Security in Development & Support Processes | Yes | No | Comment |
|-------------|--|------------|-----------|----------------|
| 10.5.1 | Are there Change Control procedures in use? | | | |
| | Do Change Control procedures apply to unplanned changes as well as planned ones? | | | |
| 10.5.2 | Is there a process for reviewing proposed changes to assess their business impact? | | | |
| | Does the review of proposed changes include consideration of how they may impact the Disaster Recovery Plan? | | | |
| 10.5.3 | Are changes to software packages discouraged unless there is a clear business or security issue? | | | |
| 10.5.4 | Are the Gaming System(s) in use by Licensee: <ul style="list-style-type: none"> • Built in-house? • Bought off-the-shelf? • Tailored from a standard package • Provided to order and to design • Other (detail) | | | |
| 10.5.5 | Where software was produced externally, has a risk assessment or ISO-17799 compliance audit been conducted on the supplier? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 11.1 | Aspects of Business Continuity Management | Yes | No | Comment |
|-------------|--|------------|-----------|----------------|
| 11.1.1 | Is there a formal, documented Business Continuity Management plan (also known as a Disaster Recovery Plan or DRP)? | | | |
| | Is the Key Official responsible for the Business Continuity Plan? | | | |
| | Are all staff aware of the contents of the Business Continuity Plan and where it can be referenced? | | | |
| 11.1.2 | Does the Business Continuity plan reflect local conditions and constraints? | | | |
| | Does the Business Continuity plan rely on switching operations to a mirror server outside Malta? | | | |
| 11.1.3 | Are Business Continuity plans tested? | | | |
| | Are tape backups or other removable media kept in Malta sufficient to restore the system locally? | | | |
| 11.1.4 | Does the Business Continuity plan allow rapid transfer of gaming activity to another jurisdiction? | | | |
| | Have Business Continuity plans been examined with a view to legal compliance with LGA and other regulations. | | | |
| 11.1.5 | Will the Business Continuity plan support all Gaming Systems at full load? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 12.1 | Compliance with Legal Requirements | Yes | No | Comment |
|--------|--|-----|----|---------|
| 12.1.1 | Has all relevant legislation been identified? Please see indicative list below and the Analytical Index of http://www2.justice.gov.mt/lom/home.asp . | | | |
| | Has responsibility for compliance been assigned? | | | |
| 12.1.2 | Is the Licensee committed to using only legitimately licensed software or freeware? | | | |
| 12.1.3 | Is there clear direction as to which records are to be kept, how long archived information should be retained and how the archive is to be protected? | | | |
| 12.1.4 | Are the Licensee's operations known to the Data Protection Registrar in Malta? | | | |
| | Does the Licensee operate in accordance with DPR concerning personal data? | | | |
| 12.1.5 | Are all users aware that unauthorised access to office systems is an offence? | | | |
| 12.1.6 | Are cryptographic controls in use considered compliant with all relevant legislation? | | | |
| 12.1.7 | Has legal advice been taken with regard to what evidence would be legally admissible in Malta where a prosecution intended in a case of fraud? | | | |

Indicative list of Maltese primary legislation which may be relevant to LGA Licensees:

- Companies Act, 1995 as amended
- Data Protection Act, 2001 as amended
- Electronic Commerce Act, 2001 as amended
- Electronic Communications (Regulation) Act, 1997 as amended
- Income Tax Act, 1948 as amended
- Income Tax Management Act, 1994 as amended
- Lotteries and other games Act, 2001 as amended (Remote Gaming Regulations)
- Prevention of Money Laundering Act, 1994 as amended

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____

| 12.2 | Review of Security Policy & Technical Compliance | Yes | No | Comment |
|-------------|---|------------|-----------|----------------|
| | Do websites relating to Gaming System(s) satisfy regulation 42? (Addiction warning) | | | |
| | Do websites relating to Gaming System(s) satisfy regulation 43? (Limits set by player) | | | |
| | Do websites relating to Gaming System(s) satisfy regulation 44? (Display of counters) | | | |
| | Do websites relating to Gaming System(s) satisfy regulation 45? (Indications of currency) | | | |
| | Do websites relating to Gaming System(s) satisfy regulation 46? (Full screens games prohibited) | | | |
| | Do websites relating to Gaming System(s) satisfy regulation 49? (Contents of homepage) | | | |
| 12.2.1 | Is there an internal audit process to assess the level of compliance with the current ISP? | | | |
| 12.2.2 | Is there an internal audit process to assess the level of technical compliance with operating procedures? | | | |
| | Has an external assessment of the Gaming System(s) vulnerabilities been conducted? | | | |
| | Are compliance reports passed to the Key Official? | | | |

| 12.3 | System Audit Considerations | Yes | No | Comment |
|-------------|--|------------|-----------|----------------|
| 12.3.1 | Is there a person appointed as Compliance Officer? | | | |
| | Is there an Internal Audit committee? | | | |
| 12.3.2 | Are software tools, data and reports kept secure? | | | |
| | Are LGA informed of the Internal Audit function? | | | |

CONFIDENTIAL

If a question appears not relevant, please put N/A (not applicable)

If a question requires further research before answering, put TBC (To Be Confirmed).

Above information provided in good faith by _____ on _____