Security audit advice

For holders of all remote gambling operator licences including specified remote lottery licences

July 2015

1 Introduction

1.1 This July 2015 advice is updated from the previously published October 2014 advice. Table 1 of the Testing strategy for compliance with the remote gambling and software technical standards (Testing strategy) sets out that an annual security audit must be carried out by an independent auditor to assess compliance against the security requirements of the Remote gambling and software technical standards (RTS). This requirement applies to licensees holding remote betting – general (but not telephone only or trading rooms), pool and intermediary, remote casino, remote bingo and remote external lottery managers and society lotteries (sales greater than £250,000 per year) licences. A copy of the audit report must be submitted to the Gambling Commission (the Commission) by the licensee annually on the anniversary of the initial audit submission.

1.2 Newly licensed remote gambling operators with one or more of the above licences must submit a security audit within six months of the granting of the licence. Where licensees do not commence trading within this period, they may apply to the Commission to submit their security audit within six months of commencing trading.

1.3 The aim of assessing compliance against these standards is to ensure that operators have appropriate security controls in place so that customers are not exposed to unnecessary risks when choosing to participate in remote gambling. The Commission requires reassurance that the information security requirements are designed to ensure important information and systems (eg personal information and customer balances; gambling transaction records and systems that decide the result of gambling) are adequately secure from attacks, tampering or information theft – either from internal or external sources.

1.4 This advice note is intended to specify the Commission's expectations for the security audit process. In summary it outlines that we expect the auditor to be independent and suitably qualified and that the scope of the audit was adequate and transparent. The audit approach and evidence measures to substantiate the results must be clear and an operator response with action plans must be included for any identified findings.

2 Security audit report content

2.1 In summary a 'good' standard security audit report must include the following:

- the operator's name
- the auditor's name and background
- the date(s) of the audit
- brief background of the operator, its business model and gambling activities offered/third parties used
- locations visited by the auditor
- the standard against which the audit was conducted, ie BS ISO/IEC 27001:2013
- an executive summary. The executive summary must include a high level overview of the work undertaken and the control environment operating. It should also include any key issues/findings

- Aside from the report detailing the assessment results for each of the RTS security elements, an auditor's opinion about whether the licensee's overall security control environment is effective for the areas outlined in the RTS must be documented (required for all audit reports conducted from 1 September 2015)
- the scope of testing (including the Information Technology systems that were reviewed)
- the audit approach (enquiry based questions, observation, evidence) key persons interviewed (this helps to identify if the appropriate persons were involved in the security audit)
- evidence obtained during the audit to substantiate audit results. This would include the documents that were reviewed (including version / dates), staff interviewed, details of the walkthroughs performed, samples reviewed to verify compliance etc.
- the results of audit (sections that are fully compliant, observation, minor non-conformity, major non-conformity)
- management plan to resolve issues that were identified
- other relevant factors such as whether the operator/systems are compliant/have been audited against other requirements, eg PCIDSS (Payment Card Industry Data Security Standards)

3 Security auditor experience

3.1 The Commission will require as part of the security audit the auditor's name and background. There must be sufficient information supplied to satisfy us that the auditor is both independent and suitably qualified.

3.2 This should include:

- the name of the audit firm and how they are suitably qualified to test compliance with BS ISO/IEC 27001:2013 (ISO 27001)
- who completed the audit, their experience and qualifications. The following certifications may demonstrate suitability to complete the audit:
  - ISO 27001 Lead Auditor
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Security Professional (CISSP)
- that they are independent of the licence holder.

3.3 A suitable auditor is likely to have completed external security audits of other organisations.

4 The scope of testing

4.1 The audit must cover Section 7 of the Testing strategy that states the following:

4.2 "The Commission has highlighted those systems that are most critical to achieving the Commission's aims and the security standards that will apply to these critical systems:

- electronic systems that record, store, process, share, transmit or retrieve sensitive customer information, eg credit/debit card details, authentication information, customer account balances
- electronic systems that generate, transmit, or process random numbers used to determine the outcome of games or virtual events
- electronic systems that store results or the current state of a customer's gambling history
- points of entry to and exit from the above systems (other systems that are able to communicate directly with core critical systems)
- communication networks that transmit sensitive customer information."

4.3 The Commission requires the auditor to detail how the critical systems were identified and if the audit included the following areas:

- applications (gambling systems)
- network (eg Windows)
- database (eg Oracle)
- operating system (eg Linux).

4.4 The scope of the audit must cover all of the RTS security elements. We recognise however that it is common audit practice to use a risk based approach and where an area has adequate previous recent external audit work or is of low risk then it may not be necessary to re-perform audit work in that area every year. For example; if a separate external audit or review of backup capability was tested in an organisation six months prior and was found to be compliant then the audit need not review that again so soon providing the auditor can review and rely on the previously conducted work. Where any aspect was not reviewed as part of this audit the report must detail why and include references to any relevant previous external audit that the auditor relied upon. Such previous audit can only be relied on if it was performed to ISO/IEC 27001 (or equivalent) standard.

5 The audit approach

5.1 The Commission must understand how the audit was conducted. It does not consider that a good audit can be conducted remotely based only on documentation. It should include all three of the below listed methods:

- asking questions (enquiry based approach)
- gathering evidence (evidence based approach)
- being on-site and speaking to staff (observation based approach).

5.2 An information security audit uses a range of assessment methods including gathering evidence, reviews of procedures, and access to offices and staff including non-technical staff eg

- HR for training records - 'RTS Annex A Security Requirement A.7.2.2 Information security awareness, education and training',
- Various managers to ensure by interview and evidence gathering that regular user access reviews are taking place - 'RTS Annex A Security Requirement A.9.2.5 Review of user access rights',
- Verifying screen locks occur on workstations after x minutes etc.

5.3 If the operator has satellite operations in a number of locations around the world then the Commission would require the operator and auditor to determine during planning which locations are most critical to visit in order to assess the information security aspects for the Commission licensed activity. Where it may not be appropriate to visit multiple locations, in certain areas remote based telephone calls and emails to gather information would suffice. A fully informed professional judgement would have to be made to ensure a suitably robust audit took place. Conducting an audit fully via remote means just by talking to staff and reviewing information by email would not be sufficient.

6 Audit coverage for aspects provided by third parties

6.1 Operators must satisfy themselves of the information security adequacy in place with the third parties they use. Social responsibility code provision 1.1.2 outlines licensees' responsibility for third parties. In addition to this code there are requirements that would be within the audit scope specifically dealing with the management of third parties (namely the ISO/IEC 27001:2013 extract within the RTS: Standard – 15 Supplier Relationships)

6.2 The auditor, as part of planning for the audit and in conjunction with the operator, must establish if there are third parties and whether they should form part of the audit scope.

Important factors to consider here would include the functions the third party performs and whether they have access to information or systems critical to the licensees' gambling provision. In some instances the auditor may be able to rely on other audit work conducted over the third party, providing the auditor is content with the adequacy and scope of that work.

6.3 A common example might be a third party data centre that hosts gambling servers. The auditor may rely on the fact that the data centre is ISO27001 certified or has been previously reviewed for the main area of their RTS responsibility (namely the physical security aspect).

6.4 Another example would be the use of B2Bs for part of the gambling provision (eg managed online slots or a poker network). In this case it is likely that the B2B is licensed as a remote gambling operator themselves and would therefore be subject to their own security audit. This fact alone does not absolve the B2C of their own responsibility in this area and we would expect the B2C to obtain assurance from the licensed B2B as outlined in 6.1. For example: contractual terms, service level agreements and assurance statements such as ISAE 3402 Statements).

7 Persons interviewed

7.1 The audit report is to include the name and title of the people that were interviewed.

7.2 The Commission would expect the key stakeholders responsible for establishing the information security framework, and applying it to be interviewed, such as:

- person with overall responsibility for remote gambling
- compliance officer
- information security officer
- operational staff (sample of)
- software developers.

8 Documents reviewed and evidence measures

8.1 The audit report must include the policies/procedures/documents reviewed. An example of some of the policies/procedures/documents that we would expect to be reviewed includes:

- IT security policy
- user access
- development and testing procedures
- service level agreement
- policy on use of network services
- detection, prevention, and recovery controls to protect against malicious code
- data backup policy
- procedures in place so that media is disposed of securely and safely
- procedures for the handling and storage of information (to protect the information from unauthorised disclosure or misuse)
- change management policy
- procedures for monitoring use of information processing facilities
- a policy, operational plans and procedures for teleworking activities
- policy on the use of cryptographic controls
- network diagram.

8.2 The operator may list different document names but this still must contain the applicable policy/procedure. The Commission may ask an operator for more information about this if it is unclear in the report.

8.3 The audit areas from which evidence is gathered includes:

- applicable security settings in place (including network, database, operating systems and gambling applications)
- user access controls (both staff and player access)
- software changes
- reviews of any externally conducted penetration testing and vulnerability assessments performed
- physical access
- audit log reviews
- information processing controls
- backup recording
- staff interviews and walkthroughs with evidence noted for selected processes
- training records.

9 Sample of audit report

9.1 The Commission would expect to receive an audit report using a standardised methodology of completing security audits. Listed below are some of the acceptable terms the Commission would expect to see in a security audit and an example of the layout of the report.

9.2 Definitions

This example report uses the following definitions for the compliance assessments of each area evaluated.

Compliant
The policy and evidence viewed was considered to be fully compliant with the BS ISO/IEC 27001:2013 guidelines.

Observation
A policy is in place but it is either not fully compliant with the BS ISO/IEC 27001:2013 guidelines or the supporting evidence (or lack thereof) raised potential concerns. This status does not signify a fail, but indicates that the process could be improved.

Minor non-conformity
A control has not been addressed or is not compliant with BS ISO/IEC 27001:2013 guidelines. A course of action to remedy this should be provided with an appropriate time line.

Major non-conformity
A fundamental failing has been identified by the auditor that affects several controls and means that the overall Information Security Management policies cannot be adhered to. Until resolved, such an issue will normally mean the organisation is not compliant with ISO/IEC 27001:2013**.**

Example of security audit and management responses to issues that were identified
The Commission recognises that all the requirements listed in Section 4 of the RTS may not apply to certain operators. Sufficient evidence must be supplied within that audit report where any requirement was not applicable.

Audit reports which do not provide sufficient and clear evidence may not meet the Commission's requirements and may be rejected.

Assessment
(Examples of content and style the Commission would expect to see.)

Reference	Requirement	Requirement	Observations / Evidence	Compliant	Observation	Minor Non-Conformity	Major Non-Conformity
A.5.1.1	Policies for information security	A set of policies for information security should be defined, approved by management, published and communicated to all employees and relevant third parties	A set of information security policies is defined and evidenced. It is published on the company intranet accessible by all employees, and communicated to all relevant third parties	x			
A.6.2.2	Teleworking	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites	No teleworking takes place within the operators business				
A.8.3.2	Disposal of media	Media should be disposed of securely when no longer required, using formal procedures	During the audit it was identified that an office computer has been replaced since the previous audit. It was confirmed by management that the old hard disk has been securely disposed by the third-party IT support company. However no documentation or certificate was provided for this process			x	

Partial and non-conformities

(Clearly defined findings assist the licensee's management and the Commission in understanding the need for taking corrective action.) In general the format of a finding should be:

- **Finding** - What was observed;
- **Objective Evidence** – Evidence that supports the finding and describes the situation that exists (finding)
- **Consequence** - Impact or potential impact of the situation that exists (finding)
- **Corrective Action** – Steps that are taken to address existing non-conformities and make improvements. They solve existing problems and should be based on the Plan, Do, Check, Act model.
- **Management response -** Outlines the management's response to findings and includes resolution dates and responsible persons.

Reference A.8.3.2	Control	Disposal of media	Status Minor Non-Conformity
Finding			
During the audit it was identified that an office computer has been replaced since the previous audit. It was confirmed by management that the old hard disk has been securely disposed by the third-party IT support company. However no documentation or certificate was provided for this process. Sufficient information should be provided to evidence this activity. There is a risk that data may be recovered following device disposal due to ineffective disposal procedures resulting in confidential information being revealed to external parties.			
Corrective Action / recommendation			
Disposal procedures should be updated to ensure that a certificate of disposal is obtained and preserved when any storage media is disposed. This will allow all assets to be clearly tracked from purchase to disposal.			
Management response: Company agrees with the recommendation and will update our disposal procedure and ensure adherence, a disposal field will be added to our asset register recording details of the disposal method, certificate reference and date.			
Resolution Date		xxxx 2015	