

Testing strategy for compliance with remote gambling and software technical standards

August 2009

1 Introduction

- 1.1** Sections 89 and 97 of the Gambling Act 2005 enable the Commission to set technical standards for remote gambling systems and gambling software respectively, to make arrangements for the administration of tests of compliance with standards and to provide for the enforcement of standards and submission to tests by attaching conditions to operating licences. Condition 2 of the Commission's *Licence Conditions and Codes of Practice (LCCP)* requires gambling software and remote operating licensees (including ancillary remote betting licensees) to comply with the Commission's technical standards and with requirements set by the Commission relating to the timing and procedures for testing.
- 1.2** This document sets out the Commission's current requirements for the timing and procedures for testing referred to in that Condition. It discusses the testing strategy for assessing compliance with the Remote Gambling and Software Technical Standards which were published in June 2007. Its publication follows discussions with operators and test houses on the Commission's proposed approach.
- 1.3** The Commission's approach to setting technical standards is outcome based to allow licensees flexibility as to the means of achieving the desired outcome. In a similar manner, the Commission takes a risk based approach to producing the testing strategy to ensure that its approach is reasonable, taking into account:
- the likelihood of non-compliance occurring
 - the impact (on customers) of non-compliance
 - the means available to assess compliance, and the likely burden imposed by the approach.
- 1.4** This document sets out:
- what the Commission would normally consider to be the types of testing required in order for it to be satisfied that the technical standards are being met
 - who the Commission considers appropriate to carry out that testing
 - the procedures for testing.
- 1.5** This is based on the potential impact of non-compliance on the customer and how obvious or easy it would be to determine whether a licensee and/or their systems are compliant.
- 1.6** There is scope for moderation or enhancement of the level of assurance required on these matters dependent on the Commission's view of the likelihood that any particular risk will crystallise for an individual licensee. The Commission will also have regard to a licensee's compliance record when determining if the current level of assurance is adequate.

2 Approach

2.1 In deciding what, and the level of, testing licensees are required to submit to we have categorised the ‘visibility’ (vis) of compliance. That is, how easy it is to see whether a system or licensee is compliant. For example, it is easy to see whether an operator has mitigated the risk that a customer will not understand the rules of the game by providing easily accessible information, whereas the underlying fairness of the game is more difficult to observe.

Table 1: How visible is compliance?

Visibility	Description
Low	Compliance is difficult to determine by external observation – functionality is within a technical solution rather than obvious procedural solution. E.g. do games operate fairly? Does the game correctly implement the rules?
Moderate	Moderately easy to spot non-compliance - eg does the operator have an internal policy and procedure that they follow or not?
High	Easy to spot non-compliance - it is obvious whether something is compliant or not. E.g. are terms and conditions accessible on a website?

2.2 We have also categorised the potential impact (imp) on the customer of non-compliance into three levels I, II, or III set out below.

Table 2: Degree of potential customer impact

Impact	Description
III	Unfair financial impact on customer(s). Potentially significant negative impact on responsible gambling. Loss of personal data.
II	Easily rectifiable financial impact (eg incorrectly settled bets). Game rules misleading to the player.
I	Inconvenience to customer(s). (Eg disabled website hyperlink. Temporary loss of access?)

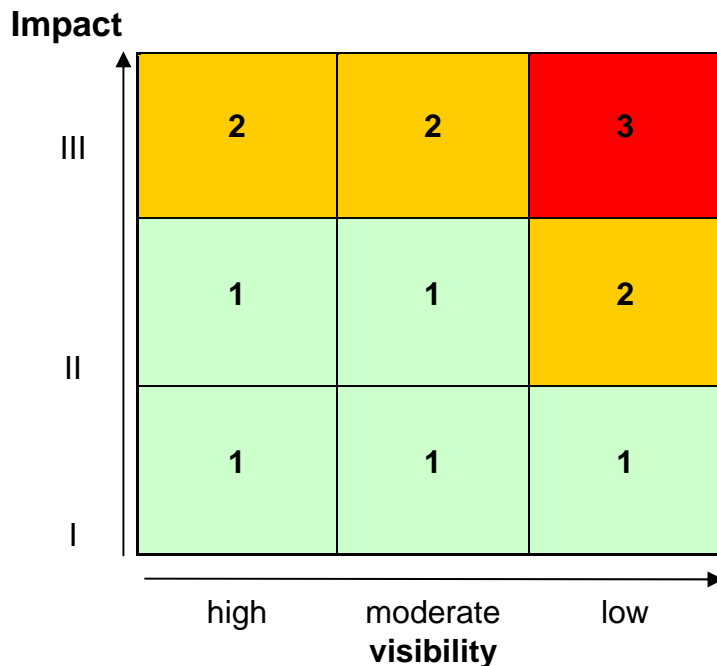
2.3 Using these criteria we have categorised the risks and associated mitigating requirements and controls into three categories (cat).

Table 3: Compliance assurance categories

Category	Assurance category description
3	Strongest degree of assurance required - normally requiring submission to a testing regime involving approved third parties.
2	Moderate amount of assurance required - normally requiring operator to present evidence that appropriate procedures are in place to assure compliance.
1	Lightest touch, compliance to be assessed by Commission, by for example, checking that operators have published the required information.

2.4 The individual technical requirements have been categorised into groups of requirements which can be treated in a similar way in terms of the category of assurance that is required and the timing of any testing or other assessment. For each group of requirements we set out the proposed type of assessment and timing of assessment.

Table 4: Mapping of risk & visibility to assurance categories



2.5 The following table sets out the Commissions current requirements. These will be kept under review.

Table 5: General risk and compliance assurance activities

General risk description	Detailed risk examples (not exhaustive)	Imp	Vis	Relevant standard	Cat	Testing required / Assurance activities
Customers are not provided with sufficient information about their gambling activity, pertinent information about the site/operator's policies, and/or the rules of the gambling.	<ul style="list-style-type: none"> Customers do not understand what they are betting on Customers are not aware of their previous betting activity Customers are not made aware of pertinent information about the site (for example, the use of automated gambling software) Customers are not made aware of the likelihood of winning Customers not easily able to keep track of their current balance. 	II	H	RTS 1A, 1B, 2A, 2B, 3A, 3B, 3C, 3D, 9A IPA 1-7	1	Commission checks for presence of required material accompanying live* gambling products, for example, on websites, mobile phones, or in printed material.
Customers suffer financial loss because the results of virtual games or other virtual events are not generated fairly.	<ul style="list-style-type: none"> Customers suffer unfair financial loss because the random number generator (RNG) is not 'random' Customers suffer unfair financial loss because scaling/mapping components do not produce the expected ('random') distribution of game outcomes. 	III	L	RTS 7A, 7B (except mechanical RNGs and lotteries that use external events)	3	Approved third party test house performs statistical analysis of RNG and game outputs, prior to release.
Customers suffer financial loss because games or virtual events contain incorrect/malicious code components that do not operate in accordance with the published rules of the game.	<ul style="list-style-type: none"> Customers suffer unfair financial loss because RNG contains incorrect/malicious code causing non-random output Customers suffer unfair financial loss because scaling and/or mapping components contain incorrect/malicious code that causes the game to operate outside the published rules. 	III	L	RTS 7A, 7B, 7C	3	Approved third party test house examines RNG, scaling and mapping components (to include source code review where considered appropriate by Commission/third party) to assess whether they operate in accordance with the rules of the virtual game or event, prior to release.

Gambling Commission – Testing strategy, remote gambling and software technical standards – August 2009

<p>Customers suffer financial loss because the results of the mechanical RNG is not fair and external events used to determine the result can be influenced.</p>	<ul style="list-style-type: none"> Customers suffer unfair financial loss because the RNG is not random Customers suffer unfair financial loss because the external event used to determine the result can be influenced. 	<p>III</p>	<p>M</p>	<p>RTS 7A (only mechanical RNG and lotteries that use external events)</p>	<p>2</p>	<p>Licensee must satisfy themselves and provide evidence that the mechanical RNG meets the guidelines set out in the standards and retain evidence to be reviewed by Commission during compliance visits.</p> <p>Lotteries will need to retain evidence that the event is external and cannot be influenced. To be reviewed by the Commission during compliance visits.</p>
<p>Customers are unfairly disadvantaged or misled by game design or functionality.</p>	<ul style="list-style-type: none"> Customers are not aware of the result of the game Customers do not know what rules apply because rules are changed during play Customers are misled about the likelihood of winning because games that appear to simulate real devices do not accurately reflect the probabilities of the real device Customers unfairly disadvantaged by games that are affected by network or end-user systems performance. 	<p>III</p>	<p>M</p>	<p>RTS 4A, 7C, 7D, 7E</p>	<p>2</p>	<p>Where relevant (eg result display duration), product testing must be conducted prior to release by licensee**. Commission will require evidence of testing to be made available.</p> <p>Internal control procedures, for example, game configuration change control, reviewed by Commission during compliance visits.</p> <p>Live* gambling products reviewed by Commission.</p>
<p>Customers are able to exploit methods of cheating and collusion to disadvantage other customers.</p>	<ul style="list-style-type: none"> Customers experience unfair financial losses because other customers cheat or collude. 	<p>III</p>	<p>M</p>	<p>RTS 11A</p>	<p>2</p>	<p>Where technical solutions are implemented, testing must be conducted prior to release by licensee**. Commission will require evidence of testing to be made available.</p> <p>Commission review and approve procedures and technical solutions intended to deter, prevent and detect cheating and collusion prior to release.</p>

Gambling Commission – Testing strategy, remote gambling and software technical standards – August 2009

Customer's gambles are not settled in accordance with the operator's rules, game rules and/or bet rules.	<ul style="list-style-type: none"> Customer suffers financial loss because bets are settled incorrectly (and not identified) or Customer is temporarily inconvenienced where bets are settled incorrectly and have to be adjusted at a later time. 	III	M	RTS 5A	2	Product testing must be conducted prior to release by licensee**. Commission will require evidence of testing to be made available.
Customers are misled about the likelihood of winning due to behaviour of play-for-fun games.	<ul style="list-style-type: none"> Play-for-fun games do not implement the same rules as the corresponding play-for-money games. 	III	M	RTS 6A	2	Product testing must be conducted prior to release by licensee** or the Commission will require evidence that the play-for-fun game is the same base game as the play-for-money game.
Customers are placed at a higher risk from irresponsible gambling because responsible gambling facilities do not work correctly or are not provided.	<ul style="list-style-type: none"> Customers who want to use some form of personal spending limit to control the amount that they gamble are unable to do so because they are not provided Customers using spending limits spend more than they intended because the limit is not properly enforced. 	III	H	RTS 12A, 12B, 13A	2	Product testing must be conducted prior to release by licensee**. Commission will require evidence of testing to be made available. Commission checks for presence of required facilities accompanying live* gambling products, for example, on websites, mobile phones, or printed material.
Customers suffer financial loss because systems are unable to adequately recover from or deal with the effects of service interruptions.	<ul style="list-style-type: none"> Customers suffer unfair financial loss because they are unable to remove a bet offer when a betting market changes Customers suffer unfair financial loss because they are unable to complete a multi-state game due to insufficient data being appropriately stored. 	III	M	RTS 10A	2	Product testing must be conducted prior to release by licensee**. Commission will require evidence of testing to be made available. Commission review technical approach and operational control procedures invoked during/after service interruptions for live* gambling products.
Customers are treated unfairly in the event of a service interruption.	<ul style="list-style-type: none"> Customers are unable to make an informed choice about whether to gamble on multi-state games or events, because the operator's policies are not published Operator policy is systematically unfair in the event of a service interruption, that is, always operates in the operators favour. 	II	H	RTS 10B	1	Commission checks that policies are easily available and accompany live* gambling products. Commission reviews service interruption policies.

Gambling Commission – Testing strategy, remote gambling and software technical standards – August 2009

<p>Customers placed at greater degree of risk from irresponsible gambling because products are designed to exploit or encourage problem gambling behaviour.</p>	<ul style="list-style-type: none"> Irresponsible product design encourages customers to gamble more than they intended or to continue gambling after they have indicated that they wish to stop Customers spend more than they intended because auto-play restrictions not in place to limit the number of transactions that can take place without customer interaction. 	<p>III</p>	<p>H</p>	<p>RTS 8A, 14A</p>	<p>2</p>	<p>Where appropriate (eg auto-play implementation), product testing must be conducted prior to release by licensee**. Commission will require evidence of testing to be made available.</p> <p>Commission review live* gambling products and may review product development policies and procedures during compliance visits.</p>
<p>Game integrity compromised because operators do not implement adequate security.</p>	<ul style="list-style-type: none"> Customers suffer unfair financial loss because weaknesses in game security are exploited. 	<p>III</p>	<p>L</p>	<p>Security</p>	<p>3</p>	<p>Annual security audit carried out by qualified and independent third party***.</p>
<p>Customer data or information is disclosed to unauthorised entities because system security is inadequate.</p>	<ul style="list-style-type: none"> Confidential customer information is disclosed to unauthorised entities leading to criminal or inappropriate use of customer information. 	<p>III</p>	<p>L</p>	<p>Security</p>	<p>3</p>	<p>Annual security audit carried out by qualified and independent third party***.</p>
<p>Customer information is lost due to inadequate security, backup or recovery provisions.</p>	<ul style="list-style-type: none"> Customers suffer unfair financial loss where the content and/or value of customer transactions (gambles) is irrecoverably lost due to inadequate system security, backup and/or recovery provisions Customers suffer unfair financial loss where customer account information is irrecoverably lost, for example, the current value of their deposits with the operator, due to inadequate system security, backup and/or recovery provisions. 	<p>III</p>	<p>L</p>	<p>Security</p>	<p>3</p>	<p>Annual security audit carried out by qualified and independent third party***.</p>

* Remote gambling products that are available to customers.

** Section 3 of this document sets out the circumstances in which operators will be permitted to carry out their own testing of gambling products.

*** Section 3 of this document explains security auditor requirements.

3 Procedure for testing

Third party test houses

- 3.1** The Commission has published a list of approved test houses that can perform third party testing. This will be updated as new test houses are approved and can be found on our website at www.gamblingcommission.gov.uk. Licensees and their chosen test house will need to agree the scope of testing and this must be sufficient to ensure that testing will adequately assess compliance with the Commission's standards.
- 3.2** Licensees must send the results of testing (ie a test house's summary report) to the Commission on completion of satisfactory testing (but prior to release). As a minimum the report should include:
- licensee name
 - date of testing
 - game details – including game name, return to player (RTP), software number and game signature
 - scope and approach to testing – for example, testing completed against the Gambling Commission's technical standards, in particular RTS 7A – 7D
 - result of testing
 - details of games/versions of games that the game supersedes
- 3.3** Once this has been provided, the successfully tested product can be released into the live environment.
- 3.4** Licensees also need to make the full test results available to the Commission on request.
- 3.5** If a licensee intends to run an off-the-shelf product (for example, a game developed by a third party software developer) they must ensure that the product is tested to confirm it meets the Commission's requirements.
- 3.6** If a third party software developer has already obtained satisfactory testing for its product by a Commission approved test house the licensee can only rely on this testing if it is able to demonstrate that the testing conducted is sufficient for the environment the product or game will operate in. If the testing obtained by the software developer is sufficient for the environment the product will operate in, the licensee must send the test house summary report to the Commission prior to release and make available full results to the Commission on request.
- 3.7** In circumstances where the operating environment differs from the testing environment the licensee will be required to obtain further testing by a test house. The Commission must receive all relevant testing reports to show the testing is sufficient to cover product or game in the operational environment prior to release. The Licensee will also need to make the full test results available to the Commission on request.
- 3.8** The licensees overall compliance with the technical standards and testing requirements (including those aspects requiring test house testing as well as internal testing) is the responsibility of the licensee.

Testing conducted by licensee/operator

- 3.9** To be permitted to carry out their own testing of gambling products licensees will be required to provide a declaration to the Commission that they follow good practice in development, testing and release control of gambling products and/or systems. More details on what the Commission considers to be good practice can be found in section 4.
- 3.10** The Commission, on request or as part of a compliance visit, may require evidence from the licensee that it complies with its good practice guidelines.
- 3.11** All results from licensee testing should be retained and be made available to the Commission during compliance visits or on request.

Third party annual security audit

- 3.12** Table 5 sets out that an annual security audit must be carried out to assess compliance against the security requirements of the remote technical standards. The security requirements are based on relevant sections of Annex A to ISO/IEC 27001:2005 and these are listed in *chapter 5 of the Remote Gambling and Software Technical Standards*. The Commission does not intend to approve security audit firms to perform the security audit as many licensees already have arrangements with appropriate security auditors.
- 3.13** However, licensees must satisfy themselves that the third party security auditor is reputable, is suitably qualified to test compliance with BS ISO/IEC 27001:2005 and that the auditor is independent from the licensee.
- 3.14** Licensees must provide to the Commission copies of the audit summary and full report produced by the security auditor on completion of their audit.
- 3.15** The Commission is aware that many operators are also subject to PCI DSS¹ and are audited for those purposes. The Commission considers its security standards to be sufficiently broad that audits conducted against other standards may meet some of the Commission's requirements. Operators will need to ensure that their audits cover the scope of the security requirements as set out in chapter 5 of the *Remote Gambling and Software Technical Standards*.
- 3.16** The Commission has highlighted those systems that are most critical to achieving the Commission's aims and the security standards 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 gamble;
 - 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.

Testing and Audit requirements for remote lottery licensees²

- 3.17** It is the Commission's view that lotteries in general pose a relatively low risk to the licensing objectives. This section sets out the criteria that applies to remote lottery licensees² (including external lottery managers) when determining specific testing and audit requirements.
- 3.18** Holders of remote lottery licences² that accept no more than £250,000 worth of entries per year by means of remote communication will not be required to submit their RNG for testing by a Commission approved test house or submit to a third party annual security audit.
- 3.19** Instead, and in terms of RNG testing, such licensees will need to demonstrate that:
- their RNG has been tested or verified as being fair and random by an independent and suitably qualified third party. This should be supported by documentary evidence
 - they have policies and procedures in place which set out how they ensure the lottery draw is fair and open and can produce evidence that these procedures are followed.

¹ (PCI DSS) Payment Card Industry Data Security Standard

² By lottery licensees we mean, remote lottery operating licensees, converted lottery operating licensees (but only those licensees that run remote lotteries themselves or via a lottery manager) or remote lottery managers' operating licensees (also know as external lottery managers)

- 3.20** In terms of the third party security audit requirement, such lottery licensees will instead be required to demonstrate to Commission compliance managers during compliance visits that they comply with the RTS security requirements as set out in *chapter 5 of the Remote Gambling and Software Technical Standards*.
- 3.21** Holders of such licences that accept more than £250,000 worth of entries by remote means per year will be required to meet the full RNG testing and third party security audit requirements as set out in table 5 above.

4 In-house development, testing and release - good practice

- 4.1** Good practice gambling software development should possess the elements below. These specific controls would already exist in an organisation compliant with ISO17799.
- 4.2** Development process:
- source code should be held in a secure environment
 - an audit log of all accesses to program source should be maintained
 - old versions of source code and the dates they were retired should be retained
 - access to source code by developers should be well controlled and based on a minimum access required for the job approach
 - access to platform source code should not be granted to those working only on game specific development
 - changes to critical modules need to be peer reviewed by appropriately skilled but independent developers to ensure all changes made are appropriate and in line with the change documentation. Any suspicious or unauthorised changes must be explained.
- 4.3** Testing Process:
- logically separate development and testing environments
 - separate staff to those that developed should perform the testing
 - an independent assessment of changes made by the developers should be performed to verify all changes are documented in the change documentation. This may involve the use of file comparison programs to quickly identify all changes.
- 4.4** Policies and processes should be in place for control of changes to operational environments including version control for software upgrades. To minimise threats to the operational environment operators should consider but not limit activities to ensuring:
- adequate testing and change control mechanisms and authorisations are in place for the migration of new or modified software into the operational environment; and
 - appropriate testing, planning and migration control measures should be carried out when upgrading patches or new software versions to ensure the overall security of the agency operational environment is not adversely impacted.

Gambling Commission August 2009

Keeping gambling fair and safe for all

For further information or to register your interest in the Commission please visit our website at: www.gamblingcommission.gov.uk

Copies of this document are available in alternative formats on request.

Gambling Commission
Victoria Square House
Victoria Square
Birmingham B2 4BP

T 0121 230 6666

F 0121 230 6720

E info@gamblingcommission.gov.uk

ADV 09/09