GAMBLING COMMISSION

Testing strategy for compliance with remote gambling and software technical standards

November 2018

Also available as webpages

Contents

1 Summary

1.1 The *Testing strategy for compliance with remote gambling and software technical standards* (the testing strategy) sets out the Gambling Commission's (the Commission's) requirements for the timing and procedures for the testing of remote gambling products (ie games and software). This sets out:

- what the Commission considers to be the types of testing required in order for it to be satisfied that the technical standards are being met
- the circumstances in which independent third party testing is required and who the Commission considers appropriate to carry out that testing
- the procedures for testing.

1.2 This is issued in accordance with sections 89 and 97 of the Gambling Act 2005 and Condition 2.3 of the Commission's *Licence conditions and codes of practice* (LCCP). The Act allows for the Commission to set technical standards and allows for administration of testing, whilst the LCCP requires relevant licensees to comply with the Commission's technical and testing requirements[1].

1.3 The Commission has an outcome based approach to compliance with its technical standards. In a similar manner, the Commission takes a risk based approach to producing the testing requirements taking into account:

- the likelihood of non-compliance occurring
- the impact of non-compliance
- the means available to assess compliance, and the burden imposed by the approach.

[1] Non-compliance with the RTS would be considered a breach of a licence condition and therefore reportable as an LCCP event notification.

Remote technical standards (RTS)

1.4 This testing strategy should be read in conjunction with the *Remote gambling and software technical standards* (RTS). The RTS can be categorised into two main areas:

1. The technical standards covering how remote gambling should be offered including the fairness of games, player account functionality and other information provision aspects.
2. Security standards covering the licensee's Information Security Management System.

1.5 While we would expect licensees to at all times ensure they are compliant with all aspects of the RTS we have designated certain aspects for which an element of independent compliance assurance is required. Table 1 sets out the level of assurance required for testing against different technical standards.

Pre-release testing and annual game testing audits

1.6 The testing strategy sets out the circumstances in which independent third party testing is required. The Commission maintains and has published a list of approved test houses that can perform third party testing. 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 and meet the level of testing required under this strategy.

1.7 For the technical standards this external assurance mainly applies to the fairness elements of RNG driven products such as casino, bingo and virtual betting. Licensees must ensure that all new products have been adequately tested by an approved test house prior to release and evidence of this (test report) has been supplied to the Gambling Commission[2].

1.8 Some retesting will be required for updates to existing games that affect a game's fairness. This strategy outlines what type of updates will generally constitute something requiring external retesting (called a major change) and what can be updated solely in reliance on internal processes and testing (minor changes).

1.9 To ensure licensees are correctly categorising changes (ie major or minor) and following defined procedures for the development, testing, release and RTP monitoring of games an annual games testing audit will be required (Section 4). This audit will be conducted by an approved test house and will apply to those licensees who develop, update and procure the external testing of RNGs and games.

Security standards – annual security audit

1.10 The information security standards are based on the international standards ISO 27001 and cover all critical gambling systems and operations. Applicable remote licensees need to undergo an annual security audit conducted by an independent and suitably qualified auditor. Results of the audit, along with a management response to any findings, need to be submitted to the Commission (Section 7).

Live dealer operations – compliance inspections

1.11 The June 2017 RTS introduced standards (RTS 17) for the operation of live dealer studios. The new requirements will apply to any live dealer licensed by us. For compliance assurance purposes, where the studio has been audited by another jurisdiction, and that audit sufficiently covers the provisions set out in RTS 17, then it won't be necessary to obtain another audit just for our purposes. If no relevant audit has been performed then one will be required to satisfy our compliance purposes.

[2] Where a licensee relies on a B2B for the provision of games they will receive a games register reference from the B2B which, once uploaded to their games register in eServices, links test reports.

2 Approach

2.1 In deciding which aspects of the RTS will require an element of independent assurance, we considered the following:

- The visibility of compliance. That is, how easy it is to see whether a system or game is compliant. For example, it is easy to see whether a licensee has mitigated the risk that a consumer 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
- Potential impact of non-compliance.

2.2 Using these criteria, Table 1 sets out the Commission's current testing strategy and is divided into two colours: green and red. These determine the risk and therefore the extent of the testing required against the relevant standard.

- Green categories contain requirements which are capable of being tested and verified by the licensee.
- Red categories contain requirements which must be assessed by a third party.

Table 1: General risk and compliance assurance activities

General risk description	Detailed risk examples (not exhaustive)	Relevant standard	Testing required/ assurance activities
Consumers are not provided with sufficient information about their gambling activity, pertinent information about the site/licensee's policies, and/or the rules of the gambling.	• Consumers do not understand what they are gambling on • Consumers are not aware of their previous gambling activity • Consumers are not made aware of pertinent information about the site (eg the use of automated gambling software) • Consumers are not made aware of the likelihood of winning • Consumers not easily able to keep track of their current balance.	RTS 1A, 1B, 1C, 2A, 2B, 2D, 3A, 3B, 3C, 3D, 4B 9A, 11B, 15A, 16A, 16B, 16C	Licensee verifies presence of required material accompanying live* gambling products, eg on websites, mobile phones, or in printed material.
Consumers suffer financial loss because the results of virtual games or other virtual events are not generated fairly.	• Consumers suffer unfair financial loss because the random number generator (RNG) is not 'random' • Consumers suffer unfair financial loss because scaling/mapping components do not produce the expected ('random') distribution of game outcomes.	RTS 7A (including mechanical RNGs except for exempt lotteries and live dealer physical devices such as roulette wheels and decks of cards)	Approved third party test house performs statistical analysis of RNG and outputs (including scaling and mapping if included within RNG), prior to release.
Consumers suffer financial loss because games, progressive jackpots or virtual events contain incorrect/malicious code components that do not operate in accordance with the published rules of the game.	• Consumers suffer unfair financial loss because scaling and/or mapping components contain incorrect/malicious code that causes the game to operate outside the published rules • Consumers suffer unfair financial loss because the actual RTP% is not in line with the expected value/s. • Consumers are misled about the likelihood of winning because games display unrealistic 'near misses', or do not accurately reflect the probabilities of simulated real devices • Consumers do not understand game operation due to the game not implementing the rules correctly, or by not displaying results clearly. • Progressive jackpot's do not increment or trigger as per the rules	RTS 7B, 7C, 7E, 9B(b) and 9B(d)	Approved third party test house examines the game (including any scaling and mapping components) via maths verification, source code analysis and game play to assess whether they operate in accordance with the rules of the virtual game or event, prior to release. RTS 3A-C and RTS 7B: While test houses aren't expected to assess how game rules are made available to players (rules easily accessible via hyperlinks etc), it is expected that they review the game display and content of player facing rules to see they accord with the maths and enable players to verify game outcomes. RTS 9 Progressive Jackpots: Test houses should verify the designs and jackpot trigger functionality to ensure it is capable of delivering the stated RTP.
Consumers' gambles are not settled in accordance with the licensee's rules, game rules and/or bet rules.	• Consumer suffers financial loss because games don't operate in accordance with the rules.	RTS 5A	In addition to pre-release in-house and any required external testing licensees must monitor the performance of games to ensure they operate in accordance with the rules. Approved third party test house assesses performance monitoring measures in place annually. Refer to Section 5 – Live RTP Monitoring.

Consumers are unfairly disadvantaged or misled by system design or functionality.	• Betting odds fluctuate after consumer request is made. • Consumers unfairly disadvantaged by games that are affected by network or end-user systems performance. • Consumers do not know what rules apply because rules are changed during play. • Progressive jackpot parameters are altered affecting RTP.	RTS 2C, 4A, 7D, 9B(a), 9B(c)	Product testing must be conducted prior to release by licensee**. Internal control procedures, for example, game configuration change control, release and performance management.
Consumers are able to exploit methods of cheating and collusion to disadvantage other consumers.	• Consumers experience unfair financial losses because other consumers cheat or collude.	RTS 11A	Where technical solutions are implemented, testing must be conducted prior to release by licensee**.
Consumers are misled about the likelihood of winning due to behaviour of play-for-free games.	• Play-for-free games do not implement the same rules as the corresponding play-for-money games.	RTS 6A	Product testing must be conducted prior to release by licensee**.
Consumers are placed at a higher risk from irresponsible gambling because responsible gambling facilities do not work correctly or are not provided.	• Consumers 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 • Consumers using spending limits spend more than they intended because the limit is not properly enforced.	RTS 12A, 12B, 13A, 13B	Product testing must be conducted prior to release by licensee**.
Consumers suffer financial loss because systems are unable to adequately recover from or deal with the effects of service interruptions.	• Consumers suffer unfair financial loss because they are unable to remove a bet offer when a betting market changes • Consumers suffer unfair financial loss because they are unable to complete a multi-state game due to insufficient data being appropriately stored.	RTS 10B	Product testing must be conducted prior to release by licensee**.
Consumers are treated unfairly in the event of a service interruption.	• Consumers are unable to make an informed choice about whether to gamble on multi-state games or events, because the licensee's policies are not published • Licensee's policy is systematically unfair in the event of a service interruption, that is, always operates in the licensees favour.	RTS 10A, 10C	Licensee verifies that policies are easily available and accompany live* gambling products. Licensee verifies performance management of system availability.
Consumers placed at greater degree of risk from irresponsible gambling because products are designed to exploit or encourage problem gambling behaviour.	• Irresponsible product design encourages consumers to gamble more than they intended or to continue gambling after they have indicated that they wish to stop • Consumers spend more than they intended because auto-play restrictions not in place to limit the number or value of transactions that can take place without consumer interaction.	RTS 8A, 8B, 14A	Where appropriate (eg auto-play implementation), product testing must be conducted prior to release by licensee**.
Consumers suffer financial loss because the results of live dealer operations are not generated fairly.	• Live dealer equipment contains bias or dealer procedures flawed resulting in unfair gambling provision.	RTS 17A	Licensees administering live dealer operations must seek independent assurance their operation conforms to requirements. Assessment to be conducted by a gambling regulator or test house.

Game integrity compromised because licensees do not implement adequate security.	• Consumers suffer unfair financial loss because weaknesses in game security are exploited.	Security	Annual security audit carried out by qualified and independent third party***.
Consumer data or information is disclosed to unauthorised entities because system security is inadequate.	• Confidential consumer information is disclosed to unauthorised entities leading to criminal or inappropriate use of consumer information.	Security	Annual security audit carried out by qualified and independent third party***.
Consumer information is lost due to inadequate security, backup or recovery provisions.	• Consumers suffer unfair financial loss where the content and/or value of consumer transactions (gambles) is irrecoverably lost due to inadequate system security, backup and/or recovery provisions • Consumers suffer unfair financial loss where consumer account information is irrecoverably lost, for example, the current value of their deposits with the licensee, due to inadequate system security, backup and/or recovery provisions.	Security	Annual security audit carried out by qualified and independent third party***.

* Remote gambling products that are available to consumers. All licensees are responsible for meeting and verifying these requirements (in Green).
** Section 6 of this document sets out the circumstances in which licensees will be permitted to carry out their own testing of gambling products.
*** Section 7 of this document explains security auditor requirements.

3 Procedure for testing

3.1 The Commission maintains and publishes a list of approved test houses authorised to perform third party testing. Licensees and their chosen test house will need to agree the scope of testing, which must be sufficient to ensure that testing will adequately assess compliance with the Commission's standards and meet the level of testing required under this strategy. This primarily applies to the RTS requirements outlined in rows 2 and 3 of Table 1 above.

3.2 Please find below level and scope of testing required by the Commission.

RNG testing:

1. Review of RNG documentation to understand the implementation of RNG in the gaming system.
2. Research about RNG algorithm/hardware to ensure there is no publicly known weakness or vulnerabilities associated with the RNG under evaluation.
3. Review of source code to verify the implementation of RNG is in accordance with the RNG documentation.
4. Statistical testing of raw output of RNG and scaled/shuffled decks data.
5. Any issues or non-compliance are reported to the supplier. Once resolved, these issues are re-evaluated to confirm the non-compliance has been addressed adequately.

Game testing:

1. Verification of game design – Maths, artwork/rules as displayed to players, and theoretical RTP.
2. Software testing - This involves verifying the software implementation of the above game design, artwork, maths and theoretical RTP through testing of the game on an environment which reflects the intended live environment; verification of game rules, actual RTP using simulation[3], emulation[4] and manual[5] testing; any scaling and mapping used to convert raw RNG output to game outcomes.

The Commission supports and participates in the International Association of Gaming Regulators (IAGR) Multi-Jurisdictional Testing Framework. This framework aims to standardise technical standards and testing requirements between participating jurisdictions in order to reduce testing duplication for products deployed internationally. Further details are available on the IAGR website.

3.3 Any additional integration testing required (for example when the game will be utilised with a different RNG or platform to the original game testing) is covered in the Gambling Platform / RNG changes below. Testing in these instances will be determined by the licensee in conjunction with the test house and will depend on the changes made to integrate the software as well as the amount of previous testing that can be relied on.

[3] **Simulation (output) testing** – setting the game up to play automatically for a high number of games (actual number will depend on volatility of the game as per the game maths) to verify that the actual RTP is within an acceptable range of the expected RTP. Sample data should be tester generated, unless supervised in a controlled environment for the purposes of meeting specific regulatory requirements. Software modified from the original to enable rapid play is permitted provided the tester has confidence that the modifications do not impact on the assessment of game fairness.

[4] **Emulation testing** is used to replicate certain rare game outcomes (such as jackpot triggers, special features and maximum prizes).

[5] **Manual game play** - actually playing the game to verify all activity observed works as expected (eg playing a game for one hour would allow the tester to see most of the common prizes and determine whether pay lines are implemented correctly etc).

3.4 For games, the testing report should include at least:

- test house details including the test supervisor that signed off the testing
- licensee name
- date of testing
- certificate reference
- game details – including game name, return to player (RTP), software number and digital signature
- scope and approach to testing and a description of all tests applied
- platform supplier and platform version
- channels (game clients) covered by testing
- result of testing
- details of games/versions of games that the game supersedes
- where a limited scope of testing has occurred due to changes within a previously tested game, an updated games test report must be provided to the Commission, making reference to the original games test report, changes made, testing completed and new digital signatures.

3.5 For RNGs, the testing report should include:

- test house details including the test supervisor that signed off the testing
- license name
- date of testing
- certificate reference
- RNG details – brief description of the RNG and its use including RNG version, whether it is hardware and/or software and digital signature
- scope and approach to testing and a description of all tests applied
- platform supplier and platform version
- Any limitations on the use of the RNG should be cited. This might include but not be limited to:
  - the acceptable degrees of freedom (DOF) permitted for the RNG,
  - whether it is suitable for use with / without replacement, and
  - any dependency on operating system functionality that if modified could impact on the operation of the RNG (eg Java SecureRandom).
- results of testing.

3.6 Licensees[6] must send the results of testing[7] (ie a test house's game/RNG report) to the Commission on completion of satisfactory testing (but prior to release). All new games and RNGs can only be released once the testing has been completed and the report provided to the Commission.

3.7 The games/RNG reports should be uploaded to the licensees games register via the eServices portal.

3.8 B2C licensees who utilise the services of a B2B for the provision of gaming content must still maintain their own up to date games register for any games offered directly or via the B2B.

[6] The following categories of licences require games and RNG testing by an independent test house (subject to a best practice declaration):
Remote general betting (standard) (virtual events), remote betting host (virtual events) remote pool betting, remote casino, remote casino (game host), remote bingo operating, remote bingo (game host) and remote lottery licences(entries greater than £250,000 per year)

[7] Where a licensee relies on a B2B for the provision of games they should receive a games register reference number from the B2B to upload the relevant game to their games register, therefore alleviating the need to re-submit the same report.

Game updates

3.9 For the purposes of this document, an update that does not impact game fairness is referred to as a minor update and can be released without the need for external retesting. For illustrative purposes, a non-exhaustive list of major/minor updates is provided in Annex A.

3.10 Licensees in conjunction with their test houses will be expected to use their own judgement as to those changes that do not affect game fairness and for all updates will need to ensure they:

- adhere to the minimum change control standards (Section 6)[8]
- maintain a record of all updates in change control documentation, which must be available upon request for inspection
- ensure a relevant personal management licence (PML) holder (or in the case of a small scale licensee, the relevant qualified person), is responsible for the process.

3.11 All of the above will be subject to an annual audit by an approved test house (Section 6).

3.12 These provisions do not affect the requirement for licensees to submit software for external testing for all new games (or updates to existing games when changes affect game fairness) and to submit the test reports (via the games register on the eServices portal) to the Commission prior to release.

Testing environment and gambling platform/RNG changes

3.13 We expect game testing to occur using the software and environment intended for live operation. Test houses would need to perform some integration testing where there are differences in the live environment compared to the test environment which could affect the fairness of games.

There are a number of games and RNGs brought under Commission regulation via transitional arrangements from other jurisdictions. Where previous testing was deemed satisfactory (previously known as level 3 testing) these games could continue to be used without need for further testing. Where the games had not been level 3 tested then further testing was required to be completed by 31 October 2015. Updates to any transitioned games should be assessed in accordance with this testing strategy (that is updates which may impact fairness need to be externally retested as per the game updates section above).

3.14 In some instances an update will be made to a remote gaming system (RGS) or an RNG which could affect the functionality, and therefore fairness, of hundreds of games served by the updated RNG or residing on the updated RGS. In this scenario licensees must ensure a representative sample of games are retested to ensure the RGS/RNG change has not affected their operation.

3.15 The sample should be wide enough to include each game type and generation (and not be restricted to RNG functionality or games with similar characteristics). The nature and size of the representative sample and the full scope of the integration testing should be decided by licensees in conjunction with an approved test house.

3.16 Details of this testing may be captured in a single test report and evidence retained by the license holder. The Commission expects testing to have been completed prior to launching the updated RNG or RGS.

[8] Section 6 sets out the minimum change control requirements that licence holders will be expected to adhere to. Licence holders may adopt alternative approaches those set out in Section 6 if they have actively taken account of the requirements and can demonstrate that an alternative approach is reasonable in the particular circumstances or that to taken an alternative approach would be acting in a similarly effective manner.

New channel testing

3.17 Where a licensee wants to release a new channel for an existing game they must ensure that channel has been tested by an approved test house. Normally, when a game is first tested for release, it will be tested using the intended channel(s) it will be offered via, for example HTML 5 and native mobile app. Over time, and as newer channels become popular, existing games may be ported across to those new channels. As the channel represents the main player interface it is important that its operation is tested.

3.18 The subset of tests for a new channel will generally be limited to the user interface and player display aspects of a game, such as a manual test to see how the game client displays results. If the backend game design and functionality have not been altered to accommodate the new channel, as is usually the case, then these aspects will not need retesting. Submission of test reports for new channels added to existing games is required, as per 3.7 above. Reference should be made to the original game test report.

3.19 Where third party client operating systems and browsers[9] are updated this generally won't require external retesting. We would expect the licensee's own testing to confirm satisfactory performance of existing games when new client operating systems and browser versions are released (note this is different to updates for the RGS or RNG, which underpins the game engine. Such updates may require games to be retested as per gambling platform/RNG changes in the above section).

3.20 Where a game is designed to work on a variety of devices or browsers testing should be of the most commonly used devices and browsers, these should be identified within the test report.

Testing and audit requirements for remote lottery licensees[8]

3.21 This section sets out the criteria that applies to remote lottery licensees[10] (including external lottery managers) when determining specific testing and audit requirements.

3.22 Holders of remote lottery licences[8] 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 undertake a third party annual security audit.

3.23 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 must 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.

3.24 In terms of the third party security audit requirement, such lottery licensees will instead be required to demonstrate to the Commission on request that they comply with the RTS security requirements as set out in Section 5 of the RTS.

---

[9] For example, updated versions of the mobile operating system provided by Apple or Google for mobile devices; or the version of the internet browser software increases.

[10] 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 known as external lottery managers) licensed under the Gambling Act 2005.

3.25 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 1 above.

4 Annual games testing audit

4.1 The requirement for an annual games testing audit applies to those licensees that hold a gambling software licence and a remote bingo operating, remote bingo (game host), remote casino, remote casino (game host), remote general betting (standard) (virtual events) or remote betting host (virtual events) Generally this will include those licensees that have assumed responsibility for games testing (eg from a software supplier or content developer).The audit must be carried out by a Commission approved test house and will:

- check a randomly selected sample of major and minor updates (to confirm that they did or did not require external testing). Section 3 and Annex A provide further detail of major/minor updates
- confirm that licence holders have adhered to required change controls (applicable elements as contained in Section 6 of the testing strategy)
- confirm the list of games made available to consumers served in reliance of a Commission licence
- confirm licensees have in place effective live RTP monitoring processes.

4.2 The above requirements set the minimum scope of the audit. The Commission may broaden the scope in c
ertain cases to address specific concerns (eg evidence of non-compliance with other aspects of the RTS/LCCP).

4.3 Where issues are identified by the audit these may be corrected by licensees, however the identified and corrected issues must still be included in the final audit report to the Commission.

4.4 The results of the audit must be counter-signed by the relevant PML holder or specified person and submitted to the Commission directly or via the approved test house that conducted the audit. It remains the responsibility of the licence holder to ensure that the audit report is submitted to the Commission. The final audit should be submitted via the eServices portal.

4.5 The audit submission dates will be staggered in order to avoid all audits being performed within a similar period and therefore putting pressure on test houses. Licensees will be assigned to a submission pool, as illustrated in Table 2 below. The Commission may be able to accommodate certain requests from licensees to be assigned to a specific pool, though this cannot be guaranteed if the allocation of the preferred audit submission pool is oversubscribed.

4.6 The Commission expects those licensees that are exempt from the annual audit requirement to seek assurance that games and updates have been tested in accordance with the testing strategy prior to release.

Table 2 Annual games testing audit submission pools

Submission pools	Audit period (previous 12 months)	Deadline for submission of annual audit to Commission
Pool 1	**1 July – 30 June following year**	**Four weeks after audit period end date**
Pool 2	**1 October – 30 September following year**	
Pool 3	**1 January – 31 December full calendar year**	
Pool 4	**1 April – 31 March following year**	

5 Live RTP monitoring

5.1 Licensees must ensure sufficient RTP monitoring is in place for both under and overpayments. The Commission expects the main form of monitoring to calculate the actual RTP and compare that figure against the expected (advertised) RTP[11].

5.2 Measurement frequency should be based on the volume of play[12]. Relying on, for example, one measurement per month will not account for particularly popular games which will accrue a high volume of play in a short time. Wherever possible measurements should be an automatic backend process that would raise alerts if actual measurements are outside the expected tolerance. One acceptable method would be to setup daily measurements based on the last 30 days of play (or other set volume(s)), in this way measurements are performed over a rolling volume of play.

5.3 Volatility is vital to these calculations regardless of volume of play and will be a key parameter to include when establishing the allowable tolerance for each game.

5.4 Monitoring must not be so aggregated that it hides errors at a lower level. For example, errors that only exist in the mobile version of the game might be less visible if monitoring aggregates all markets and channels into one calculation.

5.5 Consumers are concerned with the fairness of games and often game faults are identified as a result of their complaints. Monitoring processes should include adequate investigation of consumer complaints (especially where a game attracts more than the normal level of complaints about fairness) and ensure consumers can be provided with clear, detailed explanations of how their performance compares with the game's expected behaviour. It is not sufficient to notify players that the games have met the required testing standards as this does not acknowledge that errors can evade testing.

5.6 In scenarios where a B2B provides the games on behalf of B2Cs then live RTP monitoring would likely be performed by the B2B who holds the aggregated gaming transactions for all B2Cs. B2Cs must be made aware when incidents arise which require games offered under their licence are taken offline. New and amended contracts must make clear who is responsible for live RTP monitoring. RTP monitoring processes will be subject to the annual games testing audit. Further information of the audit is provided in Section 4 above.

[11] If the mathematical design of a game results in a theoretical RTP of 95% then a simple calculation performed using the 'win' and 'turnover' amounts generated by the game will yield the actual RTP% (win / turnover).
[12] Volume of play may be calculated based either on the number of games or amount of turnover.

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

6.1 To be permitted to carry out their own testing of gambling products licensees will be required to adhere to the below good practice guidelines in development, testing and release control of gambling products and/or systems.

6.2 Table 1 details what testing can be carried out by licensees, where a licensee does not conform with these guidelines the required testing must be carried out by an approved third party test house.

6.3 The Commission may, on request, require evidence from the licensee that it complies with these good practice guidelines. Licensees in scope for the annual games testing audit will have their controls assessed as part of that.

6.4 Controls to address the below good practice guidelines would already exist in an organisation compliant with ISO27001.

6.5 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
- Source code should be accompanied by appropriate technical documentation suitable for independent review
- all source files should contain sufficient commenting to explain file/class/function purpose
- source code should be sufficiently legible and structured to permit static code analysis and for the review of its functionality to be conducted with confidence
- write 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.

6.6 Testing process:

- logically separate development and testing environments
- separate staff to those that developed should perform the testing (in an agile development environment testing staff may be within the same team as developers testing iteratively alongside them)
- 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.

6.7 Change management:
All game and critical system changes (as defined in 7.7 below) should be supported by a change management plan which should:

- be documented
- be managed by someone with the necessary proficiency and expertise to oversee the change and make decisions
- ensure adequate testing, change control mechanisms and authorisations are in place for the software migration into the operational environment.

Accompanying any RNG/game change, the change documentation must record:

- unique change ID
- game number/RNG identifier
- delivery channel(s)
- description of change
- whether the modification is classified as major or minor
- justification for classification
- for minor changes: confirmation they have been internally tested and the changes documented
- for major changes: confirmation of adequate external testing house assessment
- relevant manager's authorisation for change
- other particulars as required by the licence holder's internal change management requirements.

7 Third party annual security audit

7.1 Table 1 sets out that an annual security audit must be carried out[13] to assess compliance against the security requirements of the RTS. The security requirements are based on relevant sections of ISO/IEC 27001:2013 and these are listed in Section 5 of the RTS. 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.

7.2 Licensees must satisfy themselves that the third party security auditor is reputable, is suitably qualified to test compliance with ISO/IEC 27001:2013 and that the auditor is independent from the licensee.

7.3 Licensees must provide to the Commission copies of the full report produced by the security auditor, along with management responses for any identified issues, on completion of their audit.

7.4 The security audit reports should be uploaded via the eServices portal.

7.5 The security auditor's report must comply with our Security audit advice.

7.6 The Commission is aware that many licensees are also subject to PCI DSS[14] 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. Licensees will need to ensure that their audits cover the scope of the security requirements as set out in Section 5 of the RTS.

7.7 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 consumer information, eg credit/debit card details, authentication information, consumer 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 consumer's gamble
- points of entry to and exit from the above systems (other systems that are able to communicate directly with core critical systems)

[13] The following categories of licences require the full security audit by an independent auditor: Remote general betting (standard) (virtual events), remote betting host (virtual events), remote pool betting, remote betting intermediary, remote bingo operating, remote bingo (host), remote casino, remote casino (game host) and remote lottery licences (entries greater than £250,000 per year).

[14] (PCI DSS) Payment Card Industry Data Security Standard.

- communication networks that transmit sensitive consumer information.

Related documents

- **Remote gambling and software technical standards, including: Security audit advice**
- **Licence conditions and codes of practice**

Annex A: Major and minor game/software updates

An update that does not impact game fairness is referred to as a minor update and can be released without the need for external retesting. The Commission have adopted a high-level principles based approach to defining major and minor updates. These principles, set out in the below table, are supported by non-exhaustive examples of major and minor updates. Licensees, in conjunction with their test houses, will be expected to use their own judgement as to those changes that do not affect game fairness.

Major change	Minor change
High level principle: A major update, which will require external retesting by an approved test house, is any software change which may affect the fairness of a game. Fairness elements would include any change to the RNG, scaling and mapping, or game rules[15] (including how the rules are processed by the software).	**High level principle:** All updates which do not fall within the definition of major update, can be dealt with as minor updates.
Non-exhaustive examples: 1. **Issue**: Inefficient logging issues causing performance impact on the game and CPU due to load. **Fix**: Amended how the game symbol arrays were constructed, allowing for faster game and reduced CPU load. *Although no rules were changed the software implementation of the rules has changed requiring independent testing*. 2. **Issue**: Bonus round win calculation update for rarely encountered scenario. **Fix**: Correct calculation in line with game design and stated rules. *This example represents an update required due to the incorrect rules implementation coding of the original release*.	**Non-exhaustive examples:** 1. **Issue**: On iOS9 updates– The sound doesn't play when spinning games when compared to iOS8 on Apple mobile devices. **Fix**: Changes to the sound format to support iOS9. *This change only impacted the games sound files. None of the game logic/maths was impacted*. 2. Display of game character hat colour and background graphics requires a change due to expiring IP rights. 3. Multiple minor issues in one update: a. Display of bonus round on screen (nothing in relation to winnings) b. Stake selection dialog in Firefox browser– not displaying fully c. URL to lobby for home button required adding d. Button display on screen slightly out of alignment. **Fix**: Most of these defects are visual issues with the game and nothing in regards to misleading players/incorrect payouts/maths changes etc. *This example could easily fall into the major change definition; where doubt exists, consultation with the original test lab would be expected.*

[15] Game rules in this context refers to the underlying maths and design of the game – pay tables, symbol distribution, feature rules etc. Collectively the game rules determine the overall game RTP. Some might also call this the game logic. It is not meant to mean that a tweak to the game rules and artwork as presented to the player (for clarification purposes) constitutes a major change.