Technical issues

Good practice guidelines for the remote gambling industry

www.rga.eu.com

RGA
remote gambling association

Contents

Introduction

1. The RGA is committed to the encouragement of high standards of probity and integrity, both for the benefit of its members and the public generally. Ensuring that technical standards are consistent, proportionate, practical, and effective is central to that, but it is also crucial to ensure the success and sustainability of all licensing regimes and the protection of consumers.

2. It would be beneficial for regulators and consumers for similar processes and standards, derived from evidence and risk based decision making, to be adopted across jurisdictions. At the moment it is common for policies to be developed in isolation, but there are increasingly calls for regulators to work together to share best practice. This was, for example, one of the recommendations in the 2011 report of the European Parliament's Internal Market and Consumer Protection Committee (IMCO) on online gambling (see Annex B for the relevant recommendations in full).

3. As the number of companies that hold licences in multiple jurisdictions increases, these inconsistencies will create more management and compliance problems and will serve to increase fragmentation of the online gambling market. It could also lead to an unnecessary duplication of company and regulatory infrastructures with replication being required in each licensing jurisdiction. Market fragmentation of this kind makes regulatory compliance less efficient; increases regulatory burden for regulators; is detrimental to consumer value; and may lead to the satisfaction of consumer demand by providers established outside the EEA area or completely un-regulated providers

4. By producing these guidelines and highlighting what it believes to be regulatory best practice, the RGA hopes that these burdens can be reduced for the benefit of all involved. In doing so it readily acknowledges the regulatory objectives of licensing jurisdictions and the work that has already been undertaken in this area by like-minded regulators through forums such as the International Association of Gaming Regulators (IAGR), and by standardisation bodies, such as the European Committee for Standardisation (CEN).

5. While innovation and technology may present new challenges for regulators, they also create new opportunities to provide efficient consumer protection and combat crime. Besides the registration of all transactions in an operator data warehouse, leaving a digital audit trail, remote gambling is characterized by increased consumer transparency and the absence of cash transactions. In addition, and notably in the field of KYC, new eVerification technologies are strategic enablers for the exclusion of under-aged people and the fight against fraud (for example, because of the decreased risk of ID theft or credit card fraud).

6. With regard to terminology, these guidelines are meant to apply, as appropriate, to all forms of remote gambling. One basic area of inconsistency that is not confined to regulators is the label attached to this sector. Apart from being called remote gambling, it is routinely referred to as online gambling, interactive gambling, egambling or a variation of those. For the purposes of this document these terms are interchangeable, except where any difference is expressly stipulated.

7. Against that background, the RGA has taken as a sensible starting point the CEN Workshop Agreement on Responsible Remote Gambling Measures (CWA 16259 January 2011) and the IAGR guidelines that were produced in 2008. It has then sought to augment them with:

    a. provisions from certain jurisdictions that license and regulate online gambling;

    b. existing legislation, notably from the EU, in the fields of consumer protection, data protection, privacy, electronic signatures and money laundering.)

    c. published material from testing houses (for example, the TST Standard Series GLI-19 31st May 2011 which also built on the pre-existing IAGR guidelines);

    d. generally accepted standards for IT governance, IT control, security and risk management (eg PCI, ITIL, COSO, ISO 27000 or the International Standards on Auditing (ISA) issued by the International Auditing and Assurance Standards Board (IAASB); and

    e. proposals for change and improvement made by interested parties from within the industry.

Objectives

8. It is intended that these guidelines should:

    a. Support regulators in designing efficient and effective technical standards within a wider regulatory framework that takes full account of information society services, consumer experience and inherent market dynamics;

    b. apply to all platforms and methods of remote delivery;

    c. accommodate the differences and the different requirements necessary between betting and gaming products;

    d. underline the integrity and fairness of remote gambling products;

    e. assist with the creation of standards that will ensure that online gambling products are fair, secure, auditable and can be regulated efficiently.

    f. provide assurance to consumers that the industry, its regulators, and those involved in testing and approving products are all committed to, and capable of, providing fair and safe betting and gaming;

    g. allow for technological developments and innovation; and

    h. cover not just the standards themselves, but also the principles of good testing of those standards by both regulators and third party testing organisations. Wherever possible they should focus on identifying what objectives they are seeking to be achieved, and not be unnecessarily prescriptive about what means should be used to achieve them.

9. It must be remembered that these guidelines are designed to represent best practice, but national and, where relevant, international laws and regulations must be taken into account and will always have precedence. This will be the case, for example, in relation to data protection, money laundering and, of course, gambling licensing requirements.

Customer registration and accounts

Display of licensed status

10. The betting and gaming websites of licensed operators must include clear statements that enable the customer to understand in which jurisdiction the particular product is licensed and regulated. They should also provide their own contact details and those for the relevant regulators.

Terms and conditions

11. Terms and conditions and general information provided to the customer must be easily accessible and stated in a clear and intelligible manner.

12. The customer registration process must include the customer's agreement to the operator's terms and conditions and customers may only be permitted to gamble if they take an action to acknowledge the agreement.

13. Where it is not possible to present the full terms and conditions to the customer at the point of registration, for example, for telephone or mobile betting, customers must be provided with easy access to the operator's terms and conditions.

System architecture and access to operator data

14. Operators will register and record all customer transactions and maintain accurate data records for the term prescribed by applicable law and licence conditions. Unless required otherwise, operators will on request make data available to the competent authorities and support any inquiry that may be conducted.

15. When considering the structure of systems and when and how to access operator data the following principles should be taken into account:

    a. Requirements should be objective and risk based. There is no need to be overly prescriptive about how policy objectives must be reached. Requirements should be technology neutral and the framework regulation should entitle the regulator to establish more detailed requirements on how objectives should be best met.

    b. High level technical requirements should be established to ensure that the game is fair and meets required quality standards. Defining high end technical requirements and duplication of IT infrastructure are two separate issues, and as in many countries the ISO 27000 standard should be used as a guideline. In this context the role of suppliers, notably software suppliers and financial service providers should be taken into consideration.

    c. Existing certifications and audit mechanisms should be recognised. Many operators will already be licensed to a high standard in in one or more credible jurisdictions. Existing audits can be purely gambling related, but may cover other aspects of a business for example, PCI audits in relation to credit card payments. Audits could be carried out by accredited third parties and above all focus on internal processes, quality control and internal control.

    d. Pragmatic Operational processes and Dynamic Change Management enable platforms to be run in an appropriate and diligent manner. Processes should be aligned with the needs of a complex and dynamic IT driven industry. Most operational changes should be subject to stringent documentation and transparency requirements allowing ex-post audit. Pre-approval of (code) change should be limited to high-risk exceptional situations, for example, when RNG or game engines are changed.

    e. Monitoring should be focussed on KPI reporting and access to source data, not localisation or duplication of IT infrastructure. The market reality of distributed IT networks of servers across multiple jurisdictions, so-called clouds or clusters (see below for more detail), render the "one local server" enforcement view outdated and ineffective. Moreover, local duplication goes against the overriding policy objectives and is often based upon a misunderstanding of relevant issues.

16. It is important to note that there is no automatic link between the location of servers and the efficient and effective regulation of the gambling activity that they support. Instead the primary focus should be on the intelligent retrieval of key information for law enforcement or compliance purposes, and less on the physical storage location. If servers are not physically situated within

a particular licensing jurisdiction, access should be provided to regulators so that they can fulfil their licensing responsibilities to the same standard as if the servers were located within their jurisdictions.

17. Where regulators require certain information to be held in a 'SAFE' (which is an operator's own data storage (a file server) where specified information about products must be held) it must be accessible online by regulators.

18. As technology evolves, the concept of a server and how it operates could change. For example, there is increasing use of distributed server networks, and in the future cloud computing could become more commonplace. It can be defined as follows:

    'Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers,storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'.
    (Meil, P., and Grance, T., The NIST Definition of Cloud Computing, Version 15, 10-07-09, available at <http://csrc.nist.gov/groups/SNS/cloud-computing/>.)

19. However, the provisions relating to adequate security, regulatory control, and access will not be affected by these changes.

Customer identification

20. A person (a "customer") should only be permitted to gamble where they hold a valid account with the operator. Verifying a customer's details is not always straightforward and so a verification period should be provided for. Within this time a customer can gamble, but cannot withdraw funds unless and until the verification is successfully completed. If the matter is not resolved at the end of that period then the account should be frozen until it is. In general, the establishment of reliable e-verification systems, provided by either the public or private sector, should be welcomed because they provide speedier and more robust processes.

21. When opening an account a customer should give as a minimum: title, name, date of birth, address where the customer is legally or normally resident, and an e mail address or equivalent means of contact such as a telephone number.

22. The operator must take reasonable steps to establish the age and identity of a person before allowing them to gamble. Confirmation and verification of that information must be undertaken before funds can be withdrawn. The means to achieve this may differ depending on the information that is available in order to check customers' age and identity in different jurisdictions, but companies should be able to take account of electronic means of identification and verification of the kind that is offered by various third party service suppliers or, in some jurisdictions, through a national database.

23. When customers have opened accounts they must only be able to access them once they have supplied or entered minimum information such as a personal user ID and password.

Record retention

24. Records of customer financial transactions and customer verification documents should be retained in accordance with the retention requirements of the operator's licensing jurisdiction.

25. All information regarding changes to customer details should be logged and the validity of requests for significant changes (e.g. changes to customers' names and banking details) should be substantiated.

Underage gambling

26. Operators must ensure that they take all reasonable steps to prevent anyone who is underage from gambling. This will generally be anyone who is under the age of 18, but that may vary between jurisdictions and sometimes between products (for example, in Britain, 16 and 17 years olds are legally permitted to gamble on National Lottery products).

27. Customers must affirm that they are of legal age to gamble as part of the registration process and the operator's website terms and conditions should state that no underage individual is permitted to participate in gambling activities.

28. The homepage of the operator's websites should prominently display an age restriction determined by its Regulatory Authority, which links through to a clear message about play by underage individuals.
29. The operator's responsible gambling page should provide a link to a recognised filtering programme to assist customers/parents in preventing underage individuals from using gambling sites.

30. If an underage player is identified after an account has been opened then the account must be suspended and any net deposits must be returned to the participants. In these circumstances the liability rests with the operator to return the funds.

31. A record of any voided transactions involving the underage player must be kept, including the reason for making the transaction void.

32. Customers must not be permitted to withdraw winnings until satisfactory completion of age verification.

Account security

33. Customers should be asked to set their own passwords, but if for any reason there is an operator generated password it must be issued securely to the customer and they should be requested to change it after they next log in.

34. The operator should advise the customer of ways they may keep their account details secure.

35. A secure process must be established for passwords to be reset/re-issued by and to customers. This process could include:

    a. requiring the customer to provide answers to "challenge questions", such as town of birth, and requiring these questions to be correctly answered before re-issuing a password or allowing a customer to choose another password;

    b. issuing the password in such a way that only the customer must have access to it, for example emailing a new password to a customer's previously nominated email address; or

    c. requiring the customer to demonstrate their identity by other means.

36. All customer accounts (including dormant accounts) must be secured against unauthorised access or change. This includes unauthorised internal access (e.g. by operator staff) and unauthorised external access (e.g. by 'hackers').

Customer accounts

37. Each customer must only be permitted to have one active account per company at a time or an operator must be able to link multiple customer accounts to that individual.

38. A new account for a person must not be created if the reason for the deactivation of a previous account indicates that the person must not be permitted to establish another account.

Customer funds controls

39. All transactions must be uniquely identifiable and maintained in a system audit log.

40. A deposit into a customer account must not be available for gambling until such time as the transaction has been approved.

41. Subject to any restrictions that may legitimately apply (ie ongoing criminal investigations or restrictions in the terms and conditions about the use of bonuses) a customer must be able to withdraw deposits from their account at any time.

42. Operators must have procedures in place to protect customer funds and they should make information available to customers about the methods they use to do so and about how they deal with unclaimed funds from dormant accounts.

Use of customer data

43. Operators must keep the customer's detailed account information (eg personal and banking details) confidential, except where the release of that information is required by law.

44. The operator must ensure that access to identifiable customer information is restricted to the customer and authorised internal staff or authorised external agencies or regulatory staff.

45. The operator must ensure that information obtained about a customer's gambling is not used to encourage compulsive gambling behaviour.

Customer consent to use of data

46. The operator's privacy policy must be stated in a clear and intelligible manner.

47. The privacy policy must inform the customer of the extent to which the operator, authorised external agencies, and regulatory staff, have access to their account information.

48. The customer registration process must include the customer's agreement to the operator's privacy policy.

49. The customer must only be permitted to gamble if they take an action to acknowledge the agreement and this arrangement should be covered in detail in the operator's privacy policy.

50. Where it is not possible to present the privacy policy to the customer at the point of registration, for example, for telephone betting, customers must be provided with easy access to the operator's privacy policy.

51. Where the operator intends to use identifiable data for purposes not directly related to the offering of a gambling product (e.g. for inclusion in a mailing list), additional specific consent must be granted by the customer. Withholding this type of consent must not be used as grounds to refuse to conduct business with a person.

Customer protection

Responsible gambling information

52. The homepage of an operator's website should contain clear links to the website of at least one organisation trained to assist problem gamblers, and a responsible gambling page containing the following:

    a. A brief statement of the operator's commitment to responsible gambling;

    b. A warning that gambling could be harmful;

    c. Advice on responsible gambling and, where available, a link to sources of help including helpline numbers;

    d. An accepted and simple self-assessment process to determine risk potential; and

    e. A list of the customer protection measures which are available on the site and details of how to access to these measures.

53. Promotional material should not be displayed on this page and any messages about an operator's support for the provision of problem gambling treatment, research, or educational initiatives should not be misleading.

54. Information concerning age limits, responsible gambling, and customer protection should be provided in each language offered by the website.

55. All links to problem gambling services provided by third parties are to be regularly tested by the operator. Where the service is no longer available, or not available for a significant period of time, the operator must provide an alternative support service.

Self-exclusion

56. Customers must be provided with an easy and obvious mechanism to self-exclude from the operator's gambling products. It must make clear to the customer the mechanism and terms on which the self-exclusion order will be implemented.

57. At a minimum, this self-exclusion mechanism must be accessible from the customer protection / responsible gambling page, or in the case of telephone gambling, by contacting the operator's customer service representatives.

58. In the case of temporary self-exclusion, the operator must ensure that:

    a. As soon as reasonably practicable following receipt of a self-exclusion order, no new bets or deposits are accepted from that customer, until such time as the temporary self-exclusion has expired;

    b. During the temporary self-exclusion period, the customer is not prevented from withdrawing any or all of their cleared account balance.

59. In the case of indefinite self-exclusion, the operator must ensure that:

    a. As soon as reasonably practicable following receipt of a self-exclusion order, no new bets or deposits are accepted from that customer;

    b. The customer's full cleared account balance is remitted to the customer using the registered name and address (except where there is suspicion or evidence of fraud or money laundering) ; and

    c. Operators must take all reasonable steps to ensure self-excluded persons are not permitted to create a new account with the operator.

    d. The self excluded person must confirm to the operator that they wish to return from a self exclusion before their account is reinstated.

60. For both temporary and indefinite self exclusions the operator must take all reasonable steps to remove the self excluded customer's details from any marketing campaigns.

Compulsory exclusion by operators

61. Where operators exclude customers they must keep a record of the reason(s) for the exclusion.

62. Immediately upon activating the exclusion, no new bets or deposits are to be accepted from that customer, until such time as the exclusion has been revoked.

63. During the exclusion period, the customer must not be prevented from withdrawing any or all of their account balance, provided that the system acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdraw (e.g. suspect of money laundering,

suspect of cheating, etc). Alternatively, and subject to the same withdrawal criteria, companies may opt to pay out any deposited funds automatically when someone decides to self exclude. It should be made clear in the company's Terms and Conditions which of these approaches it will follow.

Self-imposed limits

64. Customers must be provided with straightforward and easily accessible facilities to limit their gambling.

65. The self-limitation facilities must include at least one of the following options:

    a. Stake limit over a specified time period (e.g. daily, weekly, etc);

    b. Net loss limit per time period – an overall maximum loss limitation over a specified period of time (e.g. daily, weekly, etc);

    c. Deposit limit per time period – an overall maximum deposit limitation over a specified period of time (e.g. daily, weekly, etc) as the generally preferred method;

    d. Individual session duration limit – a limitation on the duration of each individual gambling session.

66. As soon as possible following receipt of any self-limitation request, the operator must ensure that all specified limits are correctly implemented in the system.

67. Once established by a customer, limits may only be relaxed upon 24 hours notice.

Complaints

68. Any complaints procedures must, first and foremost, be compliant with any applicable national rules under which operators are legally required to comply with.

69. Operators must provide information to customers on their website about their complaints procedure including:

    a. how to make a complaint against the operator;

    b. provision for adjudication of complaints by the regulator or approved third party; and

    c. Operators must retain customer gambling transaction data so that it:

    - complies with data retention requirements
    - enables complaints to be resolved
    - retains information that may be required for investigations by the regulator, other third party adjudicators or other approved bodies

Last log in time display

70. When a customer logs in with an operator, the last time they logged in should be displayed to the customer without the customer's intervention.

71. This is not a requirement in the case of logging in orally via telephone.

Balance display

72. Customers should be given their current account balance in currency (as opposed to credits).

73. Telephone betting customers who do not have online access to account balance information, must be provided with their balance on their request.

Customer activity statement

74. Customer activity statements must be easily available to the customer and must give sufficient information to enable them to review their previous gambling and account transactions.

75. Statements must include sufficient information to allow the customer to reconcile the statement against their own records.

76. All customer account activity information retained by the operator must be available to the customer for a reasonable timeframe.

Transaction logging

77. Transaction logging keeps a sequential record of every operation that occurs to data. Adequate on-site transaction logging of customer accounts must occur in order to ensure that dispute resolution is transparent.

Product guidance

78. This section of the guidance covers the gambling products themselves. It addresses generic issues before moving on to certain product specific measures.

Generation of random game outcomes

79. "Game outcomes" include, for example, the selection of symbols, ordering of cards, position of dice, determination of the result of a virtual race and any other events determined by reference to the output of an RNG.

80. Any RNG output used for determining game outcomes must be demonstrated to:

    a. Be statistically independent;

    b. Be uniformly distributed (within statistically expected bounds) over their range;

    c. Pass various recognised statistical tests intended to demonstrate the absence of patterns; and

    d. Be unpredictable without knowledge of the algorithm, its implementation, and the current seed value (all of which must be secure).

81. Any forms of seeding and re-seeding must not introduce predictability.

82. The range of the RNG must be sufficient to support the games that utilise its output.

83. Scaling of raw RNG outputs into specific number ranges for use in games must not introduce any bias, pattern or predictability.

84. It must be demonstrated that the method used to convert RNG output into game outcomes ("mapping") creates the expected distribution of outcome probabilities for the game.

85. Game outcomes must not be influenced, affected or controlled by anything other than RNG outputs used in accordance with the rules of the game. Note: this does not prohibit metamorphic games or jackpots determined by means other than individual game outcomes from being considered on a case-by-case basis.

86. RNG outputs must be used to generate game outcomes in the order in which they are received, in accordance with the rules of the game. Valid RNG outputs and game outcomes must not be manually or automatically discarded.

87. All RNG outcomes must be independent of previous RNG outcomes.

Mechanical RNGs

88. For games that use the laws of physics (for example, live roulette) to generate game outcomes ("mechanical RNGs") the mechanical RNG must also meet the following guideline:

    a. Components must be constructed of materials that will not degrade before their scheduled replacement lifecycle;

    b. The properties of the items used must not be altered; and

    c. Customers must not have the ability to interact with, come into physical contact with, or manipulate the components.

Software RNGs

89. Where software algorithms are used to generate random numbers the method of reseeding must be appropriate for the usage of the random numbers and ensure the software operates in a random way.

RNG failure

90. In the event of an RNG failure, games that rely upon that RNG must be made unavailable for gambling until the failure is rectified or the RNG replaced.

91. Systems, which can include automated monitoring, must be in place to identify quickly any failure of the RNG (for example, if a short sequence is repeated, or if the output is a constant flow of the same value).

Information about the generic rules for betting and gaming

92. For each game or bet, an explanation of the applicable rules must be easily available to the customer before they commit to gamble. Any changes must be date stamped and made available to the customer at all times and any changes should not be retrospective in their effect.

93. The availability of rule information must be checked regularly; where the information is not available in normal circumstances the product should not be made available for gambling.

94. The published information must be sufficient to explain all of the applicable rules.

Specific game information for remote gaming

95. As applicable, the game information must include the following minimum information:

    a. the name of the game;

    b. the applicable rules, including clear descriptions of what constitutes a winning outcome;

    c. any restrictions on play or betting, such as any play duration limits, maximum win values, etc;

    d. the number of decks or frequency of shuffles in a virtual card game;

    e. whether there are contributions to jackpots ("progressives") and the way in which the jackpot operates, for example, whether the jackpot is won by achieving a particular outcome;

    f. instructions on how to interact with the game; and

    g. any rules pertaining to metamorphosis of games, for example, the number and type of tokens that need to be collected in order to qualify for a feature or bonus round and the rules and behaviour of the bonus round where they differ from the main game.

96. For multi-state or metamorphic games, as the game progresses clear information sufficient to inform the customer about the current state of the game must be displayed on screen in text and/or artwork. For example:

    a. where a game builds up a collection of tokens (symbols, etc) the current number collected must be displayed,

    b. where different rules apply an indication of the rules that are currently relevant, such as "bonus round" or other feature labels.

97. The rules of the game must not be unfair or misleading.

98. Game rules must not be changed during a session unless adequate advance notification is given to customer.

99. Game rules must not be changed between a customer making a bet and the result of the bet being generated and calculated. For jackpots, the parameters may change once customers contribute to the jackpots. For example, at the start the full amount is used to contribute to the loan account, At a later stage the contribution amount to the loan account gets smaller and more is used for the jackpot. It does not affect the rate of the jackpot growing, but the parameters are different depending on the lifecycle of the jackpot.

Information for remote gaming about prizes and the chances of winning

100. For each game, information about the likelihood of winning must be easily available to the customer before they commit to gamble. Information must include:

    a. a description of the way the game works and the way in which winners are determined and prizes allocated, for example, for peer to peer games where the likelihood of winning is influenced by the relative skill of the participants or for Bingo where the likelihood of winning is not known at the outset because it is dependent on the number of participants, a description of the way in which prizes are won or allocated is sufficient; and

b. the theoretical return to player (RTP%) percentage which may be appropriate for a slot machine style games or other games of chance. Where games involve some element of skill the published RTP must be based on the theoretical RTP% generated by a strategy that is reasonably achievable by a customer.

101. Where games include jackpot or progressive jackpot amounts, the published information must disclose whether this is included in the overall RTP% for the game.

102. For each game, information about the potential prizes and/or payouts (including the means by which these are calculated) must be easily available. This must include, where applicable:

a. Pay tables, or the odds paid for particular outcomes;

b. For peer-to-peer games where the prize is determined based on the actions of the participants a description of the way the game works and the rake or commission charged;

c. For lotteries and other types of events where the potential amount or prize paid out may not be known before the customer commits to gamble, describing the way in which the prize amount is determined will be sufficient; and

d. displays of jackpot amounts that change over time ("progressives") must be regularly updated and as soon as possible after the jackpot has been reset following a win.

Gaming product displays

103. The name of the product must be displayed on game screens.

104. The product must display the unit and total stake for the customer's gamble including conversions to other currencies or tokens.

105. The product must display the result of every game in which the customer participates for a reasonable period of time.

106. The information displayed about the game result must be sufficient for the customer to determine whether they have lost or won and the value of any winnings.

107. The result must be displayed for a reasonable period of time, that is, sufficient time for the customer to be able to be able to understand the result of the game in the context of their gamble.

Game fairness

108. Games must operate and interact with the customer strictly in accordance with the published rules.

109. Games must not be designed in such a way as to mislead the customer about the likelihood of winning, by for example, substituting one losing outcome with another that represents a "near-miss", in order to encourage a customer to believe that they came close to winning and continue gambling.

110. Games must not be designed to give the customer the perception that skill influences the outcome of a game when it does not (i.e. where the outcome is entirely random).

111. Where a game is represented or implied to include a simulation of a real-life physical device, the behaviour of the simulation must replicate the expected behaviour of the real-life physical device. For example:

a. The visual representation of the simulation must correspond to the features of the real-life physical device;

b. The probability of any event occurring in the simulation must be equivalent to the real-life physical device (e.g. the probability of obtaining a 6 on a simulated die throw must be equal to 1 in 6);

c. Where the game simulates multiple real-life physical devices that would normally be expected to be independent of one another, each simulation must be independent of the other simulations; and

d. Where the game simulates real-life physical device that have no memory of previous events, the behaviour of the simulations must be independent of (i.e. not correlated with) their previous behaviour.

112. If a cap is established on any jackpot, all additional contributions once that cap is reached must be credited to the next jackpot.

113. If the artwork contains game instructions specifying a maximum win, then it must be possible to win this amount from a single game (including features or other game options).

114. All customers contributing to a jackpot that meet the criteria must be eligible to win the jackpot.

No adaptive behaviour by games

115. Games must not be "adaptive" or "compensated", that is, the probability of any particular outcome occurring must be the same every time the game is played, except as provided for in the (fair) rules of the game.

116. The rules of the game must not provide for manipulations of return to customer percentage based on previous turnover or money paid out, or to maintain a constant return to customer percentage.

No forced game play

117. The customer must not be forced to play a game simply by selecting it.

118. A mechanism must be implemented to prevent repeated gamble instructions, (for example, where a customer repeatedly presses "play" while waiting for a game result) to be executed

Products in multiple languages

119. Where products are provided in different language versions all product information should be available in the language chosen by the customer and the choice of language must not affect the likelihood of the customer winning.

Autoplay

120. The customer must retain control of the gambling where autoplay functionality is provided. The autoplay functionality must:

    a. enable the customer to choose the stake and either the number of auto-play gambles or the total amount to be gambled;

    b. enable the customer to stop the auto-play regardless of how many auto-play gambles they initially chose or how many remain; and

    c. not override any of the display requirements (e.g. the result of each gamble must be displayed for a reasonable length of time before the next gamble commences.

Game play

121. Customers must be provided with a facility to review the last game, either as a re-enactment or by description. The replay must clearly indicate that it is a replay of the previous game, and must provide the following information (at a minimum):

    a. The date and time the game was played;

    b. The display associated with the final outcome of the game;

    c. Total customer cash / credits at start and end of play;

    d. Amount gambled including any multipliers (e.g. number of lines played, and cash / credits bet per line);

    e. Total cash / credits won for the prize resulting from the last play (including progressive jackpots),Any customer choices involved in the game outcome; and

    f. Results of any intermediate game phases, such as gambles or feature games.

Game disable

122. It must be possible for the operator to disable any game or game session without any unfair impact on the customer.

123. The operator must provide full audit trails when disabling a game that is currently in play.

Incomplete games

124. Where a game can have multiple states, or stages, (multi-state), the system must provide a method of the customer returning to the incomplete game to complete it, without having to log off & log back on again, except for where player imposed session limits are in place. Where players are playing against each other (for example, in poker) this would not be possible and in those circumstances the rules covering time-outs and the periods permitted for reconnection must be transparent.

125. The operator must provide a mechanism for a customer to complete an incomplete game. Incomplete games may occur as a result of:

    a. Loss of communications between operator and end customer device;

    b. operator restart;

    c. Game disabled by operator;

    d. End customer device restart; and

    e. Abnormal termination of gambling application on end customer device.

126. Gambles associated with a partially complete game that can be continued must be held by the operator until the game completes.

127. The operator must ensure customer fairness, to the extent possible, in the event of a communication loss to one or more end customer devices during a multi-customer game.

128. Game rules must cater for situations where the operator loses connectivity with the customer.

Multi-customer games

129. Multi-customer games (e.g. peer to peer poker) with outcomes that can be affected through collusion between customers must not be permitted unless clear rules, compensating controls or technology is put in place to minimise the risk of cheating.

130. Multi-customer games with outcomes that can be affected through the use of automated electronic devices or ancillary computer systems must have warnings in the game rules so that customers can make an informed decision whether or not to participate.

Peer to peer gaming and the use of robots

131. Where local licensing allows for their use, when operators use programs to participate in gambling on their behalf in peer-to-peer gambling (e.g. “robots”), information must be displayed, which clearly informs customers that the operator uses this kind of software.

132. Where peer-to-peer(s) customers may be gambling against programs deployed by other customers to play on their behalf, information must be made easily available that describes that this is possible.

133. This information must warn customer of the risks of gambling against robots and of using robots themselves, that is, that the predictability of robots may be exploited by other customers.

134. If it is against the operator’s terms and conditions to use robots, information must be made easily available on how to report suspected robot use.

135. Customers must be informed where performance characteristics of networks or end-user devices may have, or may appear to have, an effect on the game, such as the display of progressive jackpot values.

Game artwork (information displayed)

136. This section refers to all forms of graphical and auditory information that is sent to the end customer device for presentation to the customer. The combination of all relevant information being presented to the customer must comply with these requirements.

137. Information published or presented to the customer in text and/or artwork must be accurate, intelligible, and unambiguous (not misleading).

138. All information presented on the website and games (whether visual or auditory, written or pictorial) must not be in any manner or form indecent, illegal or offensive (e.g. pornographic or offensive to religion or race)

139. The functions of all buttons represented on the website and games must be clearly indicated.

140. Edges of the “hot” area of buttons must be clearly defined in the artwork to prevent clicking near buttons creating a gamble.

Remote betting

Rules

141. As with all forms of gambling, comprehensive rules should be available so that there is transparency about the terms and conditions that apply when a bet is placed.

142. There may be occasions when a bet is accepted in error or on what are clearly wrong terms. This would most commonly occur if either technological or human error created an obvious pricing mistake. Information must be provided to explain how such errors will be dealt with by the operator.

Bet settlement

143. For betting, operators will need a settlement system that quickly and accurately determines the correct returns to winning customers. These systems do not have to be subject to the same testing regime as RNG driven games because they fulfil a very different function. However, a dispute resolution process should be publicly available if a customer queries any particular settlement.

Unusual and suspicious betting patterns

144. Operators should have in place mechanisms to identify unusual and suspicious betting patterns. These are necessary to protect the operator and the consumer against fraud and to assist sports in combating any threat to their integrity. Where concerns are identified they should be notified, as appropriate, to the regulator, to the relevant sports' governing body, or to a credible monitoring organization such as the European Sports Security Association (ESSA).

Information for remote betting about products and chances of winning

145. For fixed odds sports betting the prices on offer provide an immediate element of transparency and the applicable rules for different types of bet should be contained in terms and conditions.

146. For pari mutuel or 'pool' betting information should be readily available about the percentage deductions from each pool before dividends are determined.

Jackpots

Partial jackpot redirection

147. Diversion Pool schemes, where a portion of the jackpot contributions are redirected to another pool so that, when the jackpot is won, that pool is added to the restart level of the next jackpot, must be demonstrably fair. The following guidelines apply to such schemes:

    a. A jackpot redirection scheme must not have a mathematical expectation of the diversion pool of infinity; and

    b. Diversion pools must not be capped.

Multiple jackpot winners

148. The operator must address the possibility of a jackpot being won (or appearing to be won) by one or more customers at approximately the same time. The rules of the game must include resolution of this possibility.

Jackpot financial liability

149. The rules of the game must provide for any planned or unplanned termination / discontinuation of a jackpot. Of particular concern is how any outstanding jackpot pool amounts are dealt with in order to ensure customer fairness. The operator must have rules to cover the procedures to be followed if a jackpot is decommissioned by the operator to ensure that the customer is not disadvantaged.

Jackpot records

150. The operator must store and maintain the following records at a minimum:

    a. Total amount contributed / won (normally equal) for each previous jackpot, including separate figures for any diverted amounts;

    b. Grand total amount contributed / won (normally equal) for all previous jackpots combined; and

    c. Total amount contributed for current jackpot, including separate figures for any diverted amounts.

Jackpot recovery

151. In order to enable the recovery of the current value of the jackpot amount in the case of an operator failure there must be an effective and reliable disaster recovery system in place.

Liquidity

152. Adequate liquidity is necessary for the practical success of certain remote gambling products (for example, poker, bingo, and shared slot jackpots). This can require operators to pool their customers and to pool them with customers and operators in other jurisdictions.

153. Where this occurs, operators should ensure that their terms and conditions provide adequate information about the arrangements; and that all other safeguards that would normally be available (for example, consumer protection; responsible gambling provisions; and money laundering measures) are retained.

Third party product integration

154. Closely linked to liquidity is the role of networks and third party product suppliers (B2B) and their integration in the platform of gambling operators (B2C). In these circumstances the focus and onus of compliance should be on the licensed gambling operator (B2C) who the customer has an account with and who remains at all times the primary responsible person for compliance with applicable law and/or consumer protection.

155. The respective roles and responsibilities of the network/third party provider and the licensed gambling operator (who has the direct relationship with the customer) should be clearly set out by contract and the relevant terms of such a contract must be accessible to regulators. Annex C sets out where those responsibilities will normally lie.

Third party system disclosure guidelines

General statement

156. It is for individual regulators to determine what level of reliance to place on third party testing houses or on testing already undertaken by other regulators, but unnecessary duplication should be avoided.

157. Where legally required, operators must make available all results of any relevant testing (including quality assurance) and system overview diagrams.

Source code

158. For new or modified systems, RNG's or games the source code shall be commented on in an informative and useful manner and able to be installed, compiled, configured and operated. When the source code is subject to testing it should be done on a random sample basis and in conjunction with the requirements of wider Quality Assurance standards, such as ISO 9000. The following source code information must be available, but does not have to be tested:

    a. File / module / function name(s);

    b. Brief description of file / module / function purpose(s); and

    c. Edit History, including who modified it, when and why.

Documentation

159. For the base system (ie. the underlying website platform) the following documentation must be available:

    a. A list of all gambling products and individual games hosted / offered on the base website;

    b. An all-inclusive functional description of the base website (including website home page and all website peripheral pages);

    c. Detailed functional descriptions of the following processes:

        i. Customer Account Registration;
        ii. Customer Account Login (Username & Password);
        iii. Customer Interface to Customer Account;
        iv. Operator Interface to Customer Account;
        v. Operator Accounting and Financial Reporting Capabilities;

vi. Customer Protection / Exclusion Systems;
vii. Operator Payment Systems & Financial Institution Interfacing;
viii. Customer Location & Identity Verification Software; and
ix. Customer Account Deactivation.

160. For the games that run on the base system the following documentation must be available:

a. Game name;

b. Game version number(s);

c. Paytable version number(s);

d. Detailed game rules, including all options and bonus features;

e. Detailed breakdown of all paytables, payouts and mapped symbols present in the game; and

f. A formal mathematical treatise of the derivation of the theoretical Percentage Return to Player (%RTP) of the game. This information is commercially sensitive and appropriate safeguards must be in place to ensure that the regulator. or anyone authorized on behalf of the regulator, ensures its confidentiality.

161. For RNG's the following documentation must be available:

a. A list of all games connected to the RNG (including the associated mathematical Degrees of Freedom (DOFs) for each game);

b. For hardware-based RNGs:

- Type of hardware device used;
- Technical specifications for hardware device;
- Methods of connecting hardware device to operator software; and
- Details of all RNG / game implementation, including methods of scaling and mapping.

c. For software-based RNGs:

- Type of mathematical algorithm used;
- Full details, in technical terms, of random number generation process and mathematical algorithm theory;
- Details of the mathematical algorithm's period;
- Details of the mathematical algorithm's range;
- Details of the methods for seeding (and re-seeding);
- Details of the methods for background cycling / activity, and
- Details of all RNG / game implementation, including methods of scaling and mapping.

Output and control based testing

162. Although all of the above information must be available, it does not automatically have to be subject to third party testing. A control and risk-based approach with clear objectives should be taken when deciding what needs to be tested, against what standard and with the aim of addressing specific underlying policy objectives and risks.

163. Based upon best practice and international standards, the internal compliance control and risk system should include:

- The relevant compliance testing employees should be appropriately trained and aware of technical standards and internal controls.
- The internal compliance testing staff should include line items in an internal test matrix representing the consideration given to compliance with technical standards.
- All changes to the gaming system that may influence the outcome of compliance with a technical standard should follow a predefined change control process.
- The internal compliance testing staff should be responsible for testing all changes to systems that may result in non-compliance.
- No change should be implemented without internal testing and appropriate sign-off.
- Changes which result in non-compliance should be reported to the senior compliance person for re-evaluation of internal control effectiveness.

164. When a system does need to be tested, the procedures should be proportionate, and recognise the fact that all game suppliers have already gone through a process of integrity checking for the issuing of software licences.

165. Due to the dynamic nature of ICT technology, including system software components and infrastructural architecture, the most proportionate way to measure the effectiveness of those controls is to have regular checks on the real gaming system's output ("output testing"). The objective of a number of comprehensive output checks, for instance, statistical analysis or financial reconciliations, is to ensure that any electronic event offered as a gambling opportunity works as it should, is fair and operates in accordance with any stated rules. In a dynamic 24/7 ICT environment this enables continued compliance.

166. By subjecting large amounts of test data and customer log data to rigorous statistical testing and/or financial reconciliations, the integrity of gaming systems as a whole, software and its integration and interaction with other components can be confirmed. Conducting ongoing testing on the actual live gaming output of all games will verify that factors beyond the certified game source code have not influenced the fairness of games.

167. Where source code testing would be deemed of value (e.g, to ensure the quality on code line level in games):

- it should always be preceded by a review of internal quality assurance and ICT development processes, including standards such as ISO 27000 or ITIL
- take into consideration that source code testing is static, implying a code fixture , which goes against the inherent nature of a dynamic ICT environment, consumer experience and need to ensure continuous operator compliance to applicable law;
- be based upon random samples of code and not a review of all code lines
- Once the code, functionality and fairness are tested and certified, the source code for that game can be frozen through use of automated integrity checks (checksums) and classified as a certified game across multiple licensees based on an assessment of the automated integrity checks (checksums).

Security guidelines

Categories of threat

168. There are three broad categories of threats to operator's systems, these include, but are not limited to:

a. Hardware Failure – including power loss to the whole system or other disasters, hard drive failure, overheating causing shut down;

b. External Threats – from people unknown who attack the system from the outside, including DDOS attacks, Hackers, Crackers, "Social Engineering" attacks, Viruses, Worms; and

c. Internal Threats – from staff or other individuals with system access that cause damage, or loss of data through errors, ignorance of procedures, malicious intent.

Security measures

169. To minimise threats to operator's systems they must have in place security policies, procedures, and mechanisms to ensure that:

a. All sensitive customer data remains confidential and is protected from theft and misuse;

b. Generic information management security protocols, such as the ISO 27000 standard, are incorporated.

c. Customer account details are available to authorised people only;

d. The integrity of gambling and account transactions can be assured and there is an audit trail of modifications to accounts and gambling transactions;

e. Customer transactions are not lost through events such as systems failures, or unauthorised modification by entities internal or external to the operator;

f. The software that determines the results of games must be protected from unauthorised modification; and

g. These provisions should apply irrespective of the type of servers that are used (including cloud servers).

170. Security policies and procedures should be documented and communicated to relevant employees, and reviewed at least annually or in the event of material changes. These annual operator reviews should include an assessment to inform any risk-based decisions that need to be taken.

171. Internal and external security reviews, penetration testing and material changes should be conducted by appropriately qualified and experienced internal teams and should be audited annually by accredited 3rd party organisations.

172. Physical security perimeters should be in place to restrict access to authorised personnel to areas that contain information and information processing facilities and to reduce the risk of environmental threats and hazards to equipment.

173. Relevant third party and business partner contractual terms and conditions should cover all appropriate security requirements.

174. Virus scanners and/or detection programs should be installed on all pertinent information systems. These programs should be updated regularly to scan for new strains of viruses.

175. Controls should be in place to manage changes to information processing facilities and systems in order to reduce the risk of security or system failures.

176. All system users should have their identity verified with a unique account identifier/password pair, or by any other means that provide equal or greater security, prior to being permitted to access the system. All system user actions should be logged.

177. All customer deposit, withdrawal or adjustment transactions should be subject to strict security control and should be recorded in a system audit log.

178. Customer confidential information involved in online transactions should be protected by methods such as SSL to prevent incomplete transmission, misrouting, unauthorised message alteration, message interception, unauthorised disclosure, or unauthorised message duplication.

179. A policy on the use of cryptographic controls for protection of information should be developed and implemented.

Critical systems

180. As a minimum the following systems must be adequately protected:

    a. Systems that record, store, process, share, transmit or retrieve all customer information, e.g. credit/debit card details, authentication information;

    b. Systems that generate, transmit, or process random numbers used to determine the outcome of events;

    c. Systems that store the results or state of events;

    d. All points of access, either physical or electronic to any and all of the above systems (other systems that are able to communicate directly with core critical systems); and

    e. Communication networks that transmit sensitive customer information.

Detailed security guidelines

181. Operators must have an up-to-date security policy that is regularly reviewed by management.

182. Staff with direct access to critical systems must receive security training appropriate to their role.

183. Equipment used to store sensitive data must have data securely removed before disposal.

184. Equipment holding data backups must be stored securely.

185. Production and test/development facilities must be logically and/or physically separated.

186. Agreements with third parties providing hosting and/or other services to the gambling system must contain a provision for implementation of appropriate security measures

187. The operator must have policies and procedures for managing third parties and monitoring adherence to security requirements.

188. Critical systems must be protected from the unauthorised execution of mobile code. Mobile code is executable code that moves from computer to computer, including both legitimate code and malicious code such as computer viruses.

189. Adequate provision of data backups and system redundancy must be implemented to protect customers from potential financial loss due to loss of data. The systems and associated procedures must be tested regularly.

190. Networks must be adequately managed and protected from threats.

191. Appropriate network segregation must be implemented.

192. Customer confidential electronic transactions between the operators and customers, and operators and third parties passing over public networks must be protected from unauthorised message modification, disclosure, duplication or replay through methods such as SSL

193. Adequate logs for critical systems must be maintained to enable investigations to determine who did what and when, for example, amending customer balances, changing game rules or pay-tables, or administrator or root level access to critical systems.

194. Audit logs must be kept secure and protected from unauthorised access or modification.

195. Faults must be logged, analysed, and appropriate action taken to remedy them.

196. All relevant system clocks must be synchronised with an appropriate, accurate time source.

197. Users must be required to follow good practice in the selection and use of passwords.

198. Applications must implement appropriate data handling methods, including validation of input and rejection of deliberately or unintentionally corrupt data.

199. Sensitive data such as credit and debit card details and passwords must be protected from unauthorised viewing.

200. Any sensitive or confidential information maintained by the operator must be stored in areas of the system that are secured from unauthorised access, both external and internal.

Network gambling

201. All of the security and operational provisions in this guidance must also apply to the operation of networks where various companies pool their customers so they can play against each other. This might be in peer to peer gambling, such as online poker, or community gambling, such as bingo. Where gambling operators cede control to network operators of any relevant player protection mechanisms they should have in place clear contractual terms that establish what the respective responsibilities are and how they will be adhered to.

Data logging guidelines

Customer account information

202. The operator must maintain and back up the following customer account information:

    a. Customer identity details (including customer identity verification results);

    b. Account details (including changes to these details) and current balance;

    c. Any self-imposed customer protection measures (including self exclusion and self impose limits);

    d. Details of any previous accounts, including reasons for deactivation;

    e. Deposit / withdraw history; and

    f. Gambling history (i.e. games played, amounts bet, amounts won, jackpots won).

203. The operator must be capable of producing the following customer account information:

    a. active customer accounts;

    b. inactive customer accounts (including reasons for deactivation);

    c. accounts for which the customer has currently (or previously) imposed a customer protection self-exclusion;

    d. accounts for which the customer has currently (or previously) been excluded from the site by the Operator (i.e. involuntary exclusion);

    e. accounts for which the customer's funds have currently (or previously) been inactive for a defined period of time; and

    f. accounts for which one or more of the customer's deposits and / or withdraws have exceeded an Operator-configurable limit (i.e.: large deposits / withdraws). The limit must be configurable for single transactions, as well as aggregate transactions over a user-defined time period.

Gambling session information

204. The operator must maintain and back up the following gambling session information:

    a. Unique customer ID;

    b. Gambling session start and end time; and

    c. Gambling information for session (i.e. games played, amounts bet, amounts won, jackpots won, etc).

Product information

205. The operator should maintain and back up the following gaming and betting information:

    a. Unique customer ID;

    b. Unique game identifier or product and event when relating to betting;

    c. Game/event start time, according to operator;

    d. Amount wagered;

    e. Contributions to any shared pools or pots (if any) in networked or peer to peer gambling;

    f. Current game/bet status (e.g. in progress, complete, etc);

    g. Any game/event that fails to complete, and the reason why the game failed to complete);

    h. Game/event result/outcome;

    i. Jackpot wins (if any);

    j. Game/event end time, according to operator;

    k. Amount won; and

    l. An audit trail of all customer account balance changes due to a bet or a game

206. The operator must be capable of reporting the following information on current products:

    a. Game/bet name;

    b. Game/bet type;

    c. Game version number; and

    d. Game pay table details

Unusual event information

207. The operator must maintain and backup a log of all significant events on the system: including:

    a. Changes made by the Operator to game parameters;

    b. Changes made by the Operator to jackpot parameters;

    c. Irrecoverable loss of customer-related data; and

    d. Significant periods of system unavailability.

208. Where an operator uses external computer systems (ie an external RNG or suite of games) it must be able to maintain a log of significant events for those systems.

Shut down and recovery

209. Backup and recovery procedures should be in place to ensure appropriate data and information (e.g. logs and financial information) are backed up on a regular basis and can be restored in the event of a disaster.

210. Backup and disaster recovery responsibilities between software providers and operators should be clearly defined.

211. All information required for completing an incomplete game should be recoverable by the system.

212. All transactions involving customer funds should be recoverable by the system in the event of a failure or malfunction.

213. If an operator has reason to believe or to suspect that an interruption has been caused, or a transaction affected by illegal activity, the operator may withhold payment to the relevant accounts pending further investigation.

Malfunction

214. The operator's terms and conditions must clearly define the operator's policies in respect of unrecoverable malfunctions of gambling hardware / software.

215. Systems must be capable of dealing with service interruptions in a timely and effective manner.

Advertising and marketing

216. Operators should be aware of, and comply with, all statutory and other applicable rules and codes governing the advertising of gambling services and products in the jurisdictions where they are marketing.

217. An Advertising and Marketing Policy must be put in place to address the following guidelines:

    a. Advertising and Marketing must be truthful;

    b. Advertising and Marketing must not bring the Operator or the regulator into disrepute;

    c. Advertising and Marketing must not target minors (under the age of majority). Media selection, content and placement must reflect this;

    d. Advertising and Marketing must not use individuals who are, or appear to be, minors (under the age of majority) to promote gambling;

    e. Advertising and Marketing must not present winning as the most probable outcome, nor misrepresent a person's chances of winning a prize;

    f. Advertising and Marketing must not encourage excessive participation or challenge or dare people to participate;

    g. Advertising and Marketing must not encourage people to play beyond their means;

    h. Advertising and Marketing must not imply the certainty of financial reward or alleviation of personal and financial difficulties;

    i. Advertising and Marketing must not present Gambling as an alternative to employment or as a financial investment;

    j. Advertising and Marketing must not encourage play as a means of recovering past gambling or financial losses;

    k. Advertising and Marketing must not suggest that skill can influence the outcome except for where sports betting products or skill games are included, or imply that the chances of winning increase the longer one plays (outside of the factual impact of customer skill in conjunction with the rules of game play);

    l. Advertising and Marketing must not depict a pre-occupation with gambling;

    m. Advertising and Marketing must not imply or convey a message that one's status, general abilities or social success can be attributable to gambling;

    n. Where Advertising and Marketing describes prize amounts, it must describe prize amounts accurately and indicating relevant terms and conditions;

    o. Winning must not be shown out of context with the reality of the Percentage Return to Customer (%RTP) and must not promote any unrealistic expectation of winning; and

    p. Operators must ensure that they do not use customer information to market products irresponsibly.

Anti-Money Laundering (AML) guidelines

218. AML policies and procedures should cater for the identification, escalation and reporting of unusual or suspicious activities, including investigating material or unusual deposits, withdrawals and accounts where little or no gambling activity takes place. They should also take full account of specific national laws that they are subject to and of any relevant international agreements, such as the EU Money Laundering Directive.

219. As a minimum the operator's AML policies and procedures should:

    a. include the provision of suspicious transaction reports to the relevant national financial intelligence unit and international institutions;

    b. prevent deposits or payouts being made to an account (unless authorised by the AML Reporting Officer) if there is reason to suspect money laundering or terrorist activity; and

    c. allow for the use of efficient electronic verification schemes and smart technologies to detect suspicious transactions.

220. A legal disclaimer should be displayed on the operator's website stating that any criminal or suspicious activities may be reported.

221. All employees should be made aware of their personal obligations to detect and report criminal and suspicious behaviour. All employees must be aware of the dangers of 'tipping-off.' and the procedures to be followed to ensure it does not happen.

222. The operator should remit funds to the customer only to the same payment mechanism from which the funds originated, except where changes to the payment mechanism are substantiated, and where such funds are withdrawn in a licensed gambling establishment, which adheres to the relevant AML laws that are applicable in the relevant jurisdiction.

Compliance and Internal Control Systems (ICS)

223. In addition to specific obligations that might be imposed by applicable law, such as the appointment of a Money Laundering Reporting Officer (MLRO) operators should appoint suitably qualified compliance personnel, who will assume responsibility for compliance with the specified compliance controls and regulatory governance.

224. As part of its ICS AND Control Testing:

- Operators should appoint a senior compliance officer, who will assume responsibility for compliance with the specified controls.
- The compliance officer should identify the regulatory objectives of technical standards.
- The compliance officer should identify the risks that may cause non-compliance with each technical standard.
- The compliance officer should implement effective internal controls that will mitigate the risk of non-compliance.
- The compliance officer should monitor compliance and internal control effectiveness on an ongoing basis.

225. The appointed compliance personnel should ensure that: training and awareness programmes are conducted on an annual basis or more frequently if required within the operator's organisation; processes, policies and procedures required for compliance are established, implemented and maintained; and have the responsibility and authority to report on compliance to senior management.

Annex A
Glossary of terms

%RTP (see also payout percentage)
Percentage Return to Customer. The %RTP is the expected percentage of wagers that a specific game will return to the customer in the long run. The %RTP can be calculated via either a theoretical or simulated approach. The method used for calculation depends on the game type.

Account
Record kept by the operator, which shall at all times be accessible to the customer, which shows the customer's credit against the operator, including all wagers placed and all prizes won by the customer and any other debits or credits as may be permitted by the applicable terms and conditions.

ATF
Accredited Testing Facility

Background cycling / activity
If the software-based RNG is cycling in the background, it means that there is a constant string of random numbers being generated by the RNG, even if they are not actually required by the game at that time. Without background cycling / activity, one could predict the result of the next iteration of the function used to produce the random numbers if they knew the current values and the algorithm.

Base website
'Base website' refers to operator software that drives the features that are common to all of the games, such as customer account administration, website home page, website peripheral pages (e.g "Legal Disclaimer", "About Us", "FAQs", etc), and accounting and financial reporting capabilities. Any software that is not directly related to any of the games hosted / offered on the base website, and is composed of visual or auditory information that is displayed to either the customer or the Operator, is considered to be base website software.

COBIT
Control Objectives for Information and Related Technology

Control Based Testing (CBT)
Controls Based Testing is an assessment of the operational effectiveness of internal controls implemented by the licensee to prevent and detect activities that may result in non-compliance post certification. CBT should align with the Compliance and Internal Control Systems (ICS)

Chip dumping
A practice in peer-to-peer gaming (for example poker) where one customer deliberately loses to another customer in order to transfer money to that customer.

Cryptographic controls
Controls to hide or obscure the contents of information transfer or stored data, including encryption and hash functions.

DDOS
Distributed denial of service

DOF
Degree of Freedom. Equal to one less than the total number of possible outcomes (e.g. with a 52-card deck, the degrees of freedom = 51).

Dormant account
A customer account that has no transactions initiated by the customer for 12 months.

EFT
Electronic Funds Transfer

eGambling /online gambling / remote gambling
Gambling via remote means such as the internet, interactive television or mobile telephone.

EGD
Electronic Gambling Device

Emulation
All submitted games must be exhibit 'Emulation Capability' for testing purposes. This means that all games must have a mode of operation that is alternate to the standard / live version of the game (i.e. to be activated and operated in the test environment only) whereby the game outcomes can be artificially introduced into the system by the user (i.e. the tester), processed by the same game logic as the standard / live version of the game, and then displayed to the user for testing purposes.

e-verification
A process by which electronic checks can be made via databases to confirm the identity of a new customer.

FAQ
Frequently Asked Question

FATF
Financial Action Task Force

Game
'Game' refers to operator software that is specific to each individual game that is hosted / offered on the base website. Each game is to be treated as a separate and distinct entity.

IAASB
International Auditing and Assurance Standards Board

ID
Identification

Inactive customer account
Account is considered inactive when there is no customer initiated activity or contact for pre-defined period of time.

IDS
Intrusion Detection System

Internal Control System (ICS)
ICS refers to the process, functions and procedures in place within a licensed gambling operator to ensure that regulatory objectives and compliance with applicable law are achieved.

IP
Internet Protocol

ISO
International Standards Organisation

ISS
Information Systems Security. Refers to the administrative controls, technical controls and physical and environment controls necessary for the secure, safe and auditable operation of the operator by the operator.

ITIL
Information Technology Information Library – provides good practice guidelines for private and public sector IT Services Management.

LAN
Local Area Network

KPI
Key Performance Indicators

KYC
Know Your Customer

Mapping
Mapping is the process by which the scaled number is given a symbol or value that is usable and applicable to the current game (e.g. the scaled number 51 might be mapped to an ACE OF SPADES).

MCS
Monitoring and Control Systems

Metamorphic game
A game where free games, feature games or prizes (other than jackpots) are triggered by the cumulative result of a series of plays. (i.e. tokens are awarded during plays and are accumulated by players).

Money laundering
Process(es) by which criminals conceal or attempt to conceal the origin of the proceeds of their or others.' criminal activities.

MLRO
Money Laundering Reporting Officer

OS
Operating System

OSSTMM
Open Source Security Testing Methodology Manual

Output testing
Comprehensive series of testing of the integrity of the gaming system as a whole, including the integration of software and other components, and this based upon the real output of the system to ensure it works as it should. Conducting ongoing testing on the actual live gaming output of all games to verify that factors beyond the certified game source code have not influenced the fairness of games.

Payout percentage
Expected percentage of wagers a specific game will return to the customer in the long run. The payout percentage can also be calculated via either a theoretical or simulated approach.

PCI
Payment Card Industry (which has its own security standards)

Period
Period is how long before the 'random' sequence repeats. Is the output from the RNG sufficient to provide all possible outcomes? In a 52-card deck, requiring an ordered straight flush on the first hand, and assuming that one draws all ten numbers (replacements included) at the beginning of the game, the required number of ORDERED outcomes so that each outcome may be achieved is 52P10 = 5.74 X 1016. 20 balls from 80 (e.g. Keno) requires 80C20 = 3.54 X 1018 possible outcomes.

SO 27000
Specification for an Information Security Management System.

Rake
With cash game poker, players do not have to pay an entry fee to play against each other, but instead pay a 'rake' which is a commission on their winning hands.

Raw values
The unscaled output of an RNG.

Range
Range is the actual size of the output from the RNG. A 32-bit RNG provides 232 possible outcomes (4.29 X 109). If one considers a 64-bit output, one can achieve 1.8 X 1019 different RNG outcomes.

Regulatory authority
Local, regional or national authority giving explicit permission to operate one or various forms of gambling.

Reseeding
Reseeding is when the RNG algorithm is restarted (given new initial seed values).

RNG
Random Number Generator. Refers to operator hardware and / or software that determines random outcomes for use by all of the games hosted / offered on the base website.

Scaling
Raw output from an RNG will normally have a range far in excess of that required for its intended use (e.g. 32-bit RNGs have over two billion possible outcomes, but (for example) we have only to determine which of 52 cards to draw). Scaling is required to divide the raw output into smaller and usable numbers. These 'scaled' numbers can then be mapped to particular card numbers, record numbers, symbols, etc. Consequently, raw output from an RNG will sometimes have a range far smaller than that required for its intended use (e.g.: 0 < raw output < 1). In these cases, scaling is required to expand the RAW output into larger usable numbers.

Seed
The common misconception is that a seed is the INITIAL VALUE of an RNG, and once started there is no use for a seed unless the RNG is restarted. The term 'seed' is frequently misused in the case of algorithmic RNGs. For these RNGs, the seed is the value used as the basis for the next iteration of the function that forms the RNG algorithm (i.e. in most cases, the last value).

Seeding
Seeding is the method used to seed RNGs in the very first instance (i.e. upon initialisation).

Self exclusion
Process by which a customer voluntarily requests their own account be locked for a minimum period of six months in order to prevent them from further gambling with that operator during the exclusion period.

Source code testing
Technical testing of individual lines of software code to ensure the code is written in accordance with programming language standards. Source code testing does exclude the testing of the performance of the entire gaming system as such.

White label
An arrangement whereby a gambling operator hosts and provides gambling on behalf of one or more companies.

VLAN
Virtual Local Area Network

Annex B

Extracts from the European Parliament's Internal Market and Consumer Protection Committee's (IMCO) 2011 report on online gambling

10. Insists on the need to dissuade players from engaging in illegal gambling, which means that lawful services must be provided as part of a system that is coherent across Europe, especially in terms of tax treatment, and which applies common minimum standards of accountability and integrity; calls on the Commission, with due regard for the subsidiarity principle, to investigate how these common standards should be implemented, including the issue of whether a European legislative framework laying down minimum rules would be appropriate;

17. Calls on the Commission to explore - in keeping with the principle of 'active subsidiarity' - all possible tools or measures at the EU level designed to protect vulnerable consumers, prevent addiction and combat illegal operators in the field of gambling, including formalised cooperation between national regulators, common standards for operators or a framework directive; is of the opinion that a pan-European code of conduct for online gambling agreed between regulators and operators could be a first step;

29. Recommends the introduction of pan-European uniform minimum standards of electronic identification; considers that registration should be performed in such a way that the player's identity is established and at the same time it is ensured that the player has at his disposal a maximum of one gambling account per gambling company; emphasises that robust registration and verification systems are key tools in preventing any misuse of online gambling, such as money laundering;

30. Is of the opinion that in order to effectively protect consumers, especially vulnerable and young players, from the negative aspects of gambling online, the EU needs to adopt common standards for consumer protection; emphasises, in this context, that control and protection processes need to be in place before any gaming activity begins and could include, inter alia, age verification, restrictions for electronic payment and transfers of funds between gambling accounts and a requirement for operators to place notices about legal age, high-risk behaviour.

Annex C
Network gaming – definitions and who does what

Network gaming
Network gaming is remote gambling that brings players from different operators to play against each other on one network. It is generally used in peer-to-peer or community gambling such as poker or bingo – in essence one company acquires the player and another company provides the gambling. An example is where a sports betting company also wants to offer customers poker gaming but does not have enough customers to host the necessary number and variety of tables, commonly referred to as liquidity. The company will recruit players and direct them to a table hosted by a network operator. The players may be based in different jurisdictions and the gambling operators may be licensed by different regulators. The profit from the players will be split between the operator which recruits the player and the operator who provides the gaming.

Who are the participants in the network?
The **player** is the customer wanting to participate in gambling, e.g. the poker player or the bingo player.

The player provider is sometimes called a platform partner, skin operator or B2C operator. The player has their contract with the platform provider. The **platform provider** is responsible for age verification, KYC functions, registering the player and ensuring that the player is not a known money launderer/fraudster. They will also generally accept and process player deposits and makes the pay out when the player withdraws from their gambling account. They are also ultimately responsible for safeguarding the interests of the player. The platform provider may also provide "white label" services, i.e. it will provide gaming and betting services to end-consumers under a third party brand. In its product portfolio, an operator will have a number of license agreements with different providers. The gambling license held by a platform partner should cover all aspects of the customer life cycle, from registration, account opening till account closure. They would hold a remote casino operating licence if licenced in the UK.

The **network operator** or service provider is a B2B business which hosts players from the platform partners and provides the actual poker or other peer to peer gaming. The network operator is responsible for the fairness of the gambling and will also monitor the tables to ensure there is no collusion or chip dumping. Some networks will have players from just two platform partners or there may be players from many partners. Some network operators also recruit their own players. They may have a software gambling operating licence depending on where they are based (Malta class 4, Alderney Cat 2, etc.) and a remote casino operating licence if they recruit their own players. In some cases, e.g. liquidity driven games such as poker, jackpots or pool betting, the B2B supplier shall also manage and operate a network to pool liquidity. In general, the B2B product supplier acts as a "subcontractor" under the responsibility/ license of the B2C gaming operator. They will not have contact with the end-customer and is not responsible for customer protection. The B2B operator cannot provide white label services as its activities only cover product level, not customer level.

The network operator and the player provider have different roles and responsibilities. The most common of these are set out in the table below.

Responsibilities	**Platform partner** e.g. William Hill, Bet365, Unibet, Bwin.party, 888.com	**Network operator** e.g. ipoker, Microgaming, Ongame, Netent, Evolution, Gamarena	**Risk mitigation tool**
Primary responsibility	The customer - KYC, responsible gambling, game account, Anti-money laundering, fraud, complaints, etc. Gambling operator is best placed to take compliance actions based upon holistic customer view.	The gaming product - technical requirements, testing. Can assist the B2C gambling operator as second line support and this in relation to the product level only (e.g. collusion in network or bugs in software).	Contractual arrangements
Player registration	A player registers on a website and submits required player details (name, address, bank account etc.)	N/A Has no access to personal information	Remote Casino Operating licence
Age verification	Age verification checks are completed based upon information provided by the player as part of the KYC process.	N/A Has no access to personal information	Remote Casino Operating licence
Player identification verification	Player identification checks are completed based on the information provided by the player. Where possible eVerification systems should be used.	N/A Has no access to personal information	Remote Casino Operating licence
Payment system	During the registration process payment details are provided by a player (e.g. Visa card, Mastercard). Player deposits money into the gambling account held by the B2C platform partner. From that gaming account the player can withdraw funds into his bank account.	At best secondary and product level only. From the gaming account the player may transfer or deposit funds directly into their product wallet (e.g. poker) or seamless wallet (all products). From the wallet, e.g. poker wallet, the actual product gaming play will be paid. A B2C licensed operator and network operator will usually settle the net of all transactions at the end of agreed periods. In most cases this will be almost instantly based upon clearing house mechanisms. However, the B2B supplier never deals with player money directly and hence no real money is moved between the customer gaming account and the product wallet.	Contract between platform partner and network operator The platform partner is required to verify the payment details of the customer.

Responsibilities	**Platform partner** e.g. William Hill, Bet365, Unibet, Bwin.party, 888.com	**Network operator** e.g. ipoker, Microgaming, Ongame, Netent, Evolution, Gamarena	**Risk mitigation tool**
Responsible gambling	The platform provider has primary responsibility for handling any problem gambling issues that includes direct contact with the player, providing spend limits, self-exclusion and identifying potential problem gamblers. The platform provider can see some activity that may indicate problem gambling including all gambling activity for which it is fully responsible (i.e. non-poker activity). It can also see account/wallet activity that may indicate a problem e.g. a customer frequently changing credit/debit cards or increasing financial limits. The platform provider cannot see activity at the poker table (such as a player chasing losses) but can see movement of funds between the general account/ wallet into the poker wallet. To get the full picture the platform provider requires the network operator to communicate instances of suspected problem gambling behaviour at the table.	At best secondary and product level only where the B2B supplier could implement decisions made by other persons to limit or block certain products. May be able to identify player pattern that could indicate a problem gambler but does not have direct contact with a player nor know what other gambling he participates in with the platform partner. It is difficult to identify potential problem gambling on pure product level and/or act in an adequate manner. “Chasing losses”, for instance will in the end be visible also on product level, but seen a non-static concept of “problem gambling” or “risk behaviour”, product actions always have to put in the broader context.	Remote Casino Operating licence for handing problem gambling issues. Contact may include some requirement to pass player pattern information to Platform partner. For this reason, and to ensure a more efficient and holistic consumer protection standard it is recommended that limits and measures are taken on gambling operator/player account level.
Money laundering detection	The platform provider can only detect aspects under their control so may identify suspicions based on the customer due diligence checks or gambling account transactions (such as funding gambling account from one source but withdrawing to another). They cannot see if the customer was laundering money at the poker table (chip dumping) as it is only the poker network provider that has visibility of the activity at the table. The platform provider must comply with the relevant money laundering requirements of the jurisdiction they are licensed in.	At best secondary and product level only. In general, a product supplier will have little net added value it is only exposed to potential suspicious activity in the third degree (after banks and after the licensed B2C operator). In certain specific cases, review of patterns of behaviour on product level may indicate suspicious activity such as chip dumping. Most typically this will be identified via unusual betting and holding/ folding patterns. This is notably the case with poker where collusion and product fraud are more efficiently monitored by the B2B network supplier. Suppliers may be bound by different regulations for money laundering detection and reporting as they will be providing to customers in multiple jurisdictions (subject to tipping off constraints).	Remote Casino licence requires adherence to AML guidelines.

Responsibilities	**Platform partner** e.g. William Hill, Bet365, Unibet, Bwin.party, 888.com	**Network operator** e.g. ipoker, Microgaming, Ongame, Netent, Evolution, Gamarena	**Risk mitigation tool**
Handling of complaints / disputes	The platform partner will handle any first line complaints/ disputes from the customer about poker. On occasion e.g. a complaint about product play, the platform provider may ask the network operator for detailed product information.	Network gaming operator can assist with the complaints/ disputes process but does not usually have direct contact with a player.	Remote Casino Operating Licence requires platform partner to deal with complaints. The contract will specify how and on what occasions the network operator will provide information to the platform provider.
Cheating / collusion detection	Platform provider holds the personal information on their players that could assist in detecting player collusion. However this KYC information is not normally transferred to the poker network for fear of customer poaching or legal restrictions (data protection). Instead when a player is transferred to the poker network it is commonly just their user name, IP address and fund amount that is sent to the network.	Review patterns of behaviour (ideally in conjunction with the platform provider) that may indicate cheating or player collusion. This could include reviewing players' IP addresses to identify if players from same household are playing on the same tables. The same players trying to play at the one table can indicate collusion attempts. Good poker networks have sophisticated collusion detection techniques based on IP address, machine ID, user names and playing behaviour.	Remote Casino operating licence.
Facilitating game play	Primary responsibility on platform/player account level: • Platform provider must select network operators which are reputable and enter into contractual arrangements. • Platform provider remains responsible for customer and integration of product in its gaming platform.	The game is fair and played according to game rules. This would include making sure the random number generator is really random. They also administer player table allocation, player pairings and player locations. They ensure that development of games is done in accordance with certain standards/ quality assurance processes (QA). In general it is considered that actual live gaming output based testing is a more efficient and comprehensive measure of fairness than technical source code testing, which may be disproportionate in terms of objective pursued.	The platform partner is required to ensure that the gaming provided to players is fair in their operating licence.
Information security	Primary responsibility of platform provider across all segments of its operations, including on its sub-contractors. Access to player information must be appropriately controlled. Under data protection law, as harmonised in the EU, the operator will be deemed to be the "controller" and primary responsible for adherence to article 17-18 Directive 95/46/EC. In addition, the operator – who is responsible for payments – will under financial service regulations be bound to adhere to PCI-DSS standard to process credit card transactions.	Access to sensitive functionality in facilitating game play is appropriately controlled. Game data is pseudo-anonymous data as the supplier does not have KYC details. Under Data Protection law will be considered as "data processor" acting under the responsibility/instruction of the data controller/operator.	Remote Casino Operator licence. Data protection legislation.

To obtain further copies or to request a PDF version, please contact:

The Remote Gambling Association
6th Floor | 52-54 High Holborn | London WC1V 6RL | UK
www.rga.eu.com

Tel: +44 (0) 207 831 2195
Email: bwright@rga.eu.com