JERSEY GAMBLING COMMISSION

Code of Practice: Minimum Standards Applicable to Remote Gambling Operators

Adopted 2015
Revised July 2019

Table of Contents

Introduction and Overview

Traditionally, jurisdictions have taken an individual approach to their gambling law, regulation and standards. This has been successful, but has meant that companies operating in multiple jurisdictions have had to duplicate systems and testing, leading to increased costs. Consequently there has been a growing call from businesses to standardise systems and controls to increase efficiency and reduce costs. Some progress has been made in this area, with regulatory organisations like GREF, (Gaming Regulators European Forum) and IAGR (International Association of Gaming Regulators) working more in common.

The Jersey Gambling Commission ("the Commission") wishes to build on this work by clearly stating that the standards noted in this document do not necessarily have to be tested in a jurisdiction-specific manner. If an operator can show that their internal controls and testing (even to another jurisdictions' standards) meet the criteria that the JGC wishes to achieve, then the method of achieving that standard is immaterial so long as they can demonstrate that the standard has been attained. Clearly that proof must still be demonstrated, but there is flexibility as to how that can be done.

This document covers areas that the Commission needs to have explained and properly defined to show that an applicant can fulfil the licensing criteria based on the Guiding principles in the Gambling Commission (Jersey) Law 2010; namely that:

- Gambling operations must be verifiably fair
- Gambling should not be a source of crime; and that
- Gambling should not target the young or the vulnerable.

The Commission also has duties to ensure that the Island's international reputation is protected. In order to do this, the Commission has a set of high level standards of behaviour and operation that it insists all licensees comply with. The way that a company will address these, however, will vary and the Commission does not prescribe a particular methodology.

The Commission may make written exception for meeting a Standard upon sufficient justification. Guidelines are included with the Standards, and the licensee must outline compliance with the technical element in addition to mitigating risks with procedural controls. These should be detailed within the operators own Internal Operational Controls (IOC).

Testing and Audit Requirements

This document also set out the Commission's current requirements and procedures for testing. Compliance with the Standards and submitting to a testing strategy forms part of the operator's licence conditions. Importantly, it sets out the circumstances in which independent third party testing is required. Applicants should note that testing certificates submitted to satisfy the requirements of different jurisdictions may be accepted where they are considered equivalent in scope.

The strategy for compliance also sets out the independent verification requirements that licence holders must fulfil. The Commission reserves the right to vary the conditions pertaining to a licence according to the type of undertaking and product offered.

Gambling Software

In the case of gambling software, these standards apply to manufacture, supply, installation or adaptation of software for use in connection with remote gambling that takes place under an operating licence issued by the Commission.

Technical Requirements

These technical requirements seek to reduce subjective criteria in the analysis and certification of software e.g.: to only test the criteria that impacts upon the credibility and integrity of the software; to ensure that server based and server-supported games/software is fair, secure, able to be audited and operated correctly; and to recognise that non-gaming related testing is not incorporated, but left to appropriate and specialised testing laboratories.

Technology Neutral

This document remains technology neutral and does not explicitly stipulate how testing should be achieved. This document deals primarily with what is required of operators to comply with Jersey's legislation. Moreover, it does not state which testing house to use, or how to submit software for testing. It does, however, require that the operator submit software to one of the jurisdiction's approved testing laboratories.

Hosting and Branding Requirements

The objective of this requirement is to identify controls that an operator must implement as part of the hosting and branding requirements.

Hosting Requirements

The licensee must use premises that the Commission has approved by licence. The operator's IOC should clearly indicate the premises where the licensee's systems are being hosted and the approval of these premises by the Commission. Any changes to the hosting arrangement should be reflected in the IOC of the licensee, setting out the full configuration of the system, indicating where the different components of the system are being hosted and notify the Commission of such modifications.

Branding Requirements

Any full operation under a Commission licence must, within the Gaming Environment (GE) show a Jersey Gambling Commission logo, and it should be hyperlinked to the Commission's home page. Where an operator is utilising a Mirroring and Load Balancing, or Disaster Recovery licence, the recognition of the regulator in the home jurisdiction will suffice.

The operator must include within the GE at a minimum:

- The licence issuing authority;
- The licence number/identification; and
- The Commission's contact details or a link to the Commission's web site;

Customer Registration and Accounting Requirements

The objective of this requirement is to identify controls that an operator must implement as part of the customer account registration process and ongoing integrity of the account.

Terms and Conditions

1. Terms and conditions must be stated in a clear and intelligible manner.
2. The customer registration process must include the customer's agreement to the operator's terms and conditions.
3. The customer may only be permitted to gamble if they take action to acknowledge the agreement.
4. Where it is not possible to present the full terms and conditions to the customer at the point of registration, for example, for telephone betting, customers must be provided with easy access to the operator's terms and conditions.

Customer Identification

1. A person may only be permitted to gamble where they hold a valid account with a licensed operator (a "customer").
2. The operator must take reasonable steps to establish the age and identity of a person before allowing them to gamble.
3. The operator must have the capability to deny access to under-aged persons.
4. The customer must be required to demonstrate their identity in order to access the E-Gaming System (EGS) for gambling. As a minimum, this must involve the customer providing accurate credentials such as a user ID and password.
5. Appendix A of this document outlines in further detail the areas of Customer identification and verification that the JGC will focus on during both the application process and it's post licencing regulatory activity i.e. supervision and inspection.

Account Security

1. An operator generated password must be issued securely to the customer.
2. A secure process must be established for passwords to be reset/re-issued 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 should have access to it; or
   c. Requiring the customer to demonstrate their identity by other means.

3. All customer accounts (including dormant/suspended accounts) on the EGS must be secured against unauthorised access or update.
4. Where appropriate, the operator must be able to implement a user inactivity timeout that automatically logs the customer out and/or ends the customer's session after a specified period of inactivity.
5. The operator must have a way of advising the customer of ways they may keep their account details secure.

Under Age Persons

1. Persons under the age of 18 must not be permitted to gamble.
2. All gambling transactions in which a minor has participated must be made void – any amounts gambled must be returned to the participants and the fact reported to the Commission.
3. A record of any voided transactions must be kept, including the reason for making the transaction void.

Controls over Accepting Bets and Wagers

1. The operator must not offer services to a customer unless the funds necessary to cover the amount of the bet or wager are provided in a way that is acceptable and reconciled regularly.

Customer Accounts

1. Successful registration of the customer will result in the creation of a customer account unique to that individual.
2. Accounts must be secure in such a manner to prevent unauthorised access.
3. Each customer should only be permitted to have one active account at a time. If the licensee intends to allow customers to have more than one active registered account, the operator must describe the controls that mitigate the various risks stemming from the practice. The Commission expects that the licensee will address the following concerns in the analysis:
   - How the licensee structures multiple accounts (e.g. master and sub-accounts, separate wallets, linking a group of accounts, etc.).
   - How the licensee mitigates the potential for money laundering by the use of multiple accounts and diverse funding mechanisms.
   - The customer should not have the ability to play against themselves using multiple accounts.
   - Inactive accounts.
   - Demonstrate the protections for customers, particularly potential problem gamblers, or excluded customers, given that player protection

mechanisms apply to a customer, not to the account.

- The licensee should not create a new account for a customer if the reason for the deactivation of a previously registered account indicates that the customer should not be permitted to establish another account.
- If multiple account controls cannot be automated, the licensee should define alternative controls within relevant sections of the ICS, which ensure the appropriate linkage of the multiple accounts.

Customer Activity Statement

1. Customer activity statements must be easily available to the customer.
2. Statements must include sufficient information to allow the customer to reconcile the statement against their own records.

Customer Funds Controls

1. All transactions must be uniquely identifiable and maintained by and in a system producing an audit log.
2. A deposit into a customer account must not be available for betting until such time as the appropriate issuing authority has approved the transaction. This authorisation must be maintained in a system audit log and easily matched to the customer's funds.
3. A customer must be able to withdraw funds up to the current available balance on their account at any time, subject to any reasonable AML controls.
4. A documented process must be put in place to deal with unclaimed funds from dormant accounts; and the Commission must approve this process.
5. Each customer's funds are separately recorded from other customer's funds and from the funds of the operator.
6. Any unplayed funds of a customer that are held by the operator are kept separate from the operating funds of the operator and may not be used by the operator, any creditors of the operator or any holding body or subsidiary of the operator.

Customer Game Session

1. The operator must give the customer an electronic identifier such as a digital certificate or an account description and a password to establish a session.
2. A session finishes if:
    - The customer notifies the operator that the session is finished (i.e. logs out),
    - A customer-inactivity timeout is reached,
    - The Operator terminates the session under approved circumstances (e.g. agreed session time limit is reached).

Handling and Use of Customer Data

The objective of this requirement is to identify those controls an operator should implement to protect customer data from misuse. This includes access to customer data and the requirements that should be outlined in an operator’s privacy policy.

Policy

1. The operator must have a privacy policy posted on the web site and accessible from the customer protection / responsible gambling page.

Use of Data

1. The operator must keep the customer’s account information confidential, except where the release of that information is required by law.
2. The operator must ensure that access to customer registration is restricted to the customer and authorised internal personnel or the Commission’s staff only.
3. The operator must ensure that information obtained about a customer’s gambling behaviour is not used to encourage irresponsible gambling.
4. The operator must be registered under the Data Protection Law of the jurisdiction.

Customer Consent to Use of Data

1. The operator’s privacy policy must be stated in a clear and intelligible manner.
2. The privacy policy must inform the customer that the operator and the Commission have access to their account information.
3. The customer registration process must include the customer’s agreement to the operator’s privacy policy.
4. The customer may only be permitted to gamble if they take an action to acknowledge the agreement.
5. 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.
6. Where the operator intends to use data for purposes not directly related to the offering of a gambling product (e.g. for inclusion in a mailing list), the customer must grant additional specific consent. Withholding this type of consent may not be used as grounds to refuse to conduct business with a person.

Cookies

Where cookies are used by the EGS, customers must be informed of the usage.

Customer Protection

The objective of this requirement is to identify controls that an operator should implement in the area of customer protection. This includes a mechanism for making a complaint against the operator; a process to self-exclude from an operator's gambling facilities and the means to implement self-imposed limits on gambling. This also includes links to help and advice on problem gambling.

Please refer to the Commission Code on Social Responsibility for Remote Operators.

General

1. Customer protection / responsible gambling information should be easily accessible. As a minimum, entry windows (entry pages or screens) must contain a link to the operator's responsible gambling and/or customer protection information.
2. As a minimum, the following information must be made available:
    - Advice that the site provides information on problem gambling and a link to that advice.
    - A list of the customer protection / responsible gambling facilities available to the customer (e.g. session time limits, bet limits, etc.), and a link to those facilities or instructions on how to access those facilities.
    - An easy and obvious mechanism to advise the customer of the right to make a complaint against the operator, and to enable the customer to notify the Commission for making such a complaint. This must include a link to information on how to contact the Commission.
    - Explanation of website filtering and blocking.
3. All account-related windows (particularly the deposit window) must provide a readily accessible link to the customer protection / responsible gambling information and a link to a reputable problem gambling service that has agreed to be linked to the site. Operator's must select a problem gambling service and notify that to the Commission.
4. 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.

Last Log in Date and Time Display

1. When a customer logs into the EGS, the last time they logged in must be displayed to the customer without the customer's intervention.

Balance Display

1. Current account balance must be displayed in local currency (as opposed to credits).

Self-Exclusion

1. Customers must be provided with an easy and obvious mechanism to self-exclude.
2. At a minimum, this self-exclusion mechanism must be accessible from the

customer protection / responsible gambling page, or by the operator's customer service representatives.

3. In the case of temporary self-exclusion, the operator must ensure that:
    - Immediately upon receiving the self-exclusion order, no new bets or deposits are accepted from that customer, until such time as the temporary self-exclusion has expired, and
    - During the temporary self-exclusion period, the customer is not prevented from withdrawing any or all of their cleared account balance.
    - The self-excluded person must confirm to the operator that they wish to return from a self-exclusion before their account is re-instated.
    - In the event that a player chooses to self-exclude for a period up to or greater than six months the operator must contact them and offer links to help providers for problem gambling.
4. Self-excluded persons must not be permitted to create new accounts with the operator during the self-exclusion time Note: See customer accounts part 3 for more information.
5. In the case of permanent self-exclusion, the operator must ensure that:
    - Immediately upon receiving the self-exclusion order, no new bets or deposits are accepted from that customer
    - The customer's full cleared account balance is remitted to the customer using the registered name and address.
    - The account is then closed.

Involuntary Exclusion

1. Where an operator excludes a customer they must keep a record of the reason(s) for the exclusion (e.g. harassing help-desk staff, harassing other customers, etc).
2. 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 or has ended.
3. 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 withdrawal (e.g. suspect of cheating, etc…)

Self-Limitation

1. Customers must be provided with straightforward and easily accessible facilities to limit their gambling.
2. The self-limitation facilities must include, but not necessarily be limited to, the following options:
    a) Spend limit over a specified time period (e.g. daily, weekly, etc),
    b) 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),

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

e) Cumulative session duration limit per time period – a limitation on the length of time a customer may gamble within a specified time period.

3. Immediately upon receiving any self-limitation order, the operator must ensure that all specified limits are correctly implemented in the system.
4. Once established by a customer, limits may only be relaxed upon 24 hours notice.
5. Limits must not be compromised by external time events, such as leap years and daylight savings adjustments.
6. Limits must not be compromised by internal status events, such as self-exclusion requests.

Involuntary Limitation

1. Operators may set their own customer limits.
2. Customers must be informed of any such limits.
3. The lower of the two limits must always apply.

Transaction Logging

1. Adequate on-site transaction logging of customer accounts must occur in order to ensure that dispute resolution is transparent (for detailed requirements, please refer to **Data Logging Requirements** section of this document).
2. Adequate backups of customer account transactions must occur in order to ensure all customer account balances can be recovered in the event of a disaster rendering the EGS inoperable (for detailed requirements, please refer to **Data Logging Requirements** section of this document).

Malfunction

1. The operator's terms and conditions must clearly define the operator's policies in respect of unrecoverable malfunctions of gambling hardware / software.
2. Systems must be capable of dealing with service interruptions.

Generation of Random Outcomes

The objective of this requirement is to ensure that the results of a game are randomly generated and the game operates in accordance with the rules.

Controls should also be in place to identify and rectify a RNG failure if this were to occur. This ensures that the integrity of gambling is not compromised.

General

"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 a Random Number Generator (RNG).

1. Any RNG output used for determining game outcomes must be demonstrated to:
   - Be statistically independent,
   - Be uniformly distributed (within statistically expected bounds) over their range,
   - Pass various recognised statistical tests intended to demonstrate the absence of patterns, and
   - Be unpredictable without knowledge of the algorithm, its implementation, and the current seed value (all of which must be secure).
2. Any forms of seeding and re-seeding must not introduce predictability.
3. The range of the RNG must be sufficient to support the games that utilise its output.
4. Scaling of raw RNG outputs into specific number ranges for use in games must not introduce any bias, pattern or predictability.
5. 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.
6. 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.
7. 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 may not be manually or automatically discarded.

Hardware RNGs

1. For games that use a *hardware* RNG to generate game outcomes the RNG must also meet the following requirements:

- Components must be constructed of materials that will not degrade before their scheduled replacement lifecycle,
- The properties of the items used should not be altered,
- Customers must not have the ability to interact with, come into physical contact with, or manipulate the components.

Software RNGs

1. Where software algorithms are used to generate random numbers the method of reseeding must be appropriate for the usage of the random numbers, for example, reseeding must take place before the RNG output pattern repeats, that is: the reseeding frequency must be shorter than the RNG period.

RNG Failure

1. 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.
2. Systems must be in place to quickly identify 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.
3. Adequate transaction logging must be in place in order to ensure that the RNG failure can be identified and that the resolution is transparent (for detailed requirements, please refer to **Data Logging Requirements** section of this document).

Game Requirements

The objective of this requirement is to identify controls that an operator should implement to ensure that a game is conducted in a way that is fair to the player.

The player should have confidence that the game is being conducted fairly and in accordance with the rules. It should be clear to the player the amount that is being gambled, the rules that pertain to the game or wagers and the result of the game or wagers.

Standard of information

1. Information published or presented to the customer in text and/or artwork must be accurate, intelligible, unambiguous and not misleading.
2. 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. sex or sexuality should not be used to promote gambling products).

General information

1. Where 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.
2. 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. If it is against the operator’s terms and conditions to use robots, the information must include how to report suspected robot use. This information must warn customers of the risks of gambling against robots and of using robots themselves, namely, that other customers may exploit the predictability of robots.
3. 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.

Information about the rules of the game

1. For each game, an explanation of the applicable rules must be easily available to

the customer before they commit to gamble.

2. The availability of game rules must be checked regularly; where the information is not available the game must not be made available for gambling.
3. The published game information must be sufficient to explain all of the applicable rules and how to participate.
4. As applicable, the game information must include the following minimum information:
    - the name of the game;
    - the applicable rules, including clear descriptions of what constitutes a winning outcome;
    - any restrictions on play or betting, such as any play duration limits, maximum win values, etc;
    - the number of decks or frequency of shuffles in a virtual card game;
    - 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;
    - instructions on how to interact with the game;
    - 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.
5. 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:
    - where a game builds up a collection of tokens (symbols, etc) the current number collected must be displayed,
    - where different rules apply an indication of the rules that are currently relevant, such as "bonus round" or other feature labels.
6. The rules of the game must not be unfair or misleading.
7. Game rules must not be changed during a session unless adequate advance notification is given to customer (where customers have incomplete games, etc)
8. Game rules must not be changed between a customer making a bet and the result of the bet being generated and calculated. For jackpots, parameters may not be altered once customer(s) have contributed to the jackpot.

Information about prizes and the chances of winning

1. 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 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;
- house edge (or margin), for example, the typical margin for a virtual horse race, where games involve an element of skill the published Return to Player percentage ("RTP%") must be based on the theoretical RTP% generated by a strategy that is reasonably achievable by a customer;
- the RTP%, which may be appropriate for slot machine style games. 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; or
- the probability (likelihood) of winning events occurring, which may be appropriate for "fixed-odds-betting" style games, where the RTP% is not necessarily informative.

2. Where games include jackpot or progressive jackpot amounts, the published information must disclose whether this is included in the overall RTP% for the game.
3. For each game, information about the potential prizes and/or payouts, or the means by which these are calculated, must be easily available, including, where applicable:

    - Pay-tables, or the odds paid for particular outcomes.
    - For peer-to-peer games where the prize is determined and based on the actions of the participants a description of the way the game works and the rake or commission charged.
    - 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.
    - displays of jackpot amounts that change over time ("progressives") must be updated at least every 30 seconds and as soon as possible after the jackpot has been reset following a win.

Play for fun games

1. Play-for-fun games must accurately represent the play-for-money version of the game; in particular they must not be designed to mislead the customer about the likelihood of winning in the play-for-money version of the game by, for example, using mappings that produce different outcome likelihoods.

Game displays

1. The name of the game must be displayed on game screens.
2. The game must display the unit and total stake for the customer’s gamble.
3. The game must display the result of every game in which the customer participates.
4. 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.
5. The result must be displayed for a reasonable period of time, that is, sufficient time for the customer to be able to understand the result of the game in the context of their gamble.

Game Fairness

1. Games must operate and interact with the customer strictly in accordance with the published rules.
2. Games must not be designed in such a way as to mislead the customer about the likelihood of winning, 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.
3. 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. the outcome is entirely random).
4. Where a game is represented or implied to include a simulation of a real-life physical device, the behaviour of the simulation must be identical to the expected behaviour of the real-life physical device. That is:
    - The visual representation of the simulation must correspond to the features of the real-life physical device,
    - The probability of any event occurring in the simulation must be equivalent to the real-life physical devices (e.g. the probability of obtaining a 6 on a simulated die throw must be equal to 1 in 6),
    - 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
    - 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.
5. The Commission reserves the right to restrict games if it determines the rules to be unfair.
6. If a cap is established on any jackpot, all additional contributions once that cap is reached must be credited to the next jackpot.
7. 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).

8. All customers contributing to a jackpot must be eligible to win the jackpot.

Adaptive Behaviour by Games

1. Games should not ordinarily 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.
2. Where a game is compensated then this must be expressly stated so that players cannot be confused between the nature of a compensated versus a random game.

No Forced Game Play

1. The customer must not be forced to play a game simply by selecting it.
2. A mechanism must be implemented to prevent repeated "gamble" instructions from being executed, e.g. where a customer repeatedly presses "play" while waiting for a game result.

Games in multiple languages

1. The following principles must be followed where games are provided in different language versions:
    - All game information must be provided in the language specified for that version,
    - The game instructions (and restrictions) must carry the same meaning across all language versions so that no one version is advantaged or disadvantaged, and
    - Customers must have the same likelihood of winning regardless of which language version they choose to play.

Game Design

1. Auto-play functionality should be devised to ensure that the customer is still in control of the gambling. Additionally, auto-play should comply with the following:
    - The customer should choose the stake and either the number of auto-play gambles or the total amount to be gambled
    - During auto-play the customer should be able to stop the auto-play regardless of how many auto-play gambles they initially chose or how many remain.
    - Auto-play should 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.

2. All critical functions, including the generation of the outcome of any game (and resultant RTP%), must take place in the EGS servers not on the end user device.

3. Game outcome determination must not be affected by the effective bandwidth, link utilisation, bit error rate or other characteristic of the communications channel between the operator and the end customer device.

Game Play

1. If the operator extends an invitation to participate in a particular game, it must accept all legitimate wagers (as defined in the rules) for that game.
2. 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):
    - The date and time the game was played;
    - The display associated with the final outcome of the game, either graphically or via a clear text message;
    - Total customer cash / credits at start of play;
    - Total customer cash / credits at end of play;
    - Amount bet including any multipliers (e.g. number of lines played, and cash / credits bet per line);
    - Total cash / credits won for the prize resulting from the last play (including progressive jackpots);
    - Any customer choices involved in the game outcome;
    - Results of any intermediate game phases, such as gambles or feature games.

Game Disable

1. It must be possible for the operator to disable any game, that is, it must be possible to prevent all customers from playing a particular game.
2. When a game is disabled, all customers playing that game must be permitted to conclude their current game session.
3. The operator must provide full audit trails when disabling a game that is currently in play.
4. The operator must also provide a mechanism for each active game session on the system to be disabled, individually, by the operator – with full consideration to the associated requirements listed above.

Incomplete Games

1. Where a game can have multiple states, or stages, (multi-state), the system must provide a method for the customer returning to the incomplete game to complete it, without having to log off & log back on again.
2. The operator must provide a mechanism for a customer to complete an incomplete game before a customer is permitted to participate in any other game. Incomplete games may occur as a result of:

- Loss of communications between operator and end customer device,
- operator restart,
- Game disabled by operator,
- End customer device restart, and
- Abnormal termination of gambling application on the end customer device.

3. Upon reconnection by the customer, the operator must present the customer the incomplete game for completion.
4. Multi-state games that have been disabled by the operator may be terminated immediately, and the stake returned to the customer.
5. The operator must hold bets associated with a partially complete game that can be continued until the game is completed. Customer accounts must reflect any funds held in incomplete games.
6. Game rules must specify that bets placed but remaining undecided in incomplete games will become void after 90 days, unless otherwise agreed with the Commission.

Multi-Customer Games

1. Multi-customer games (e.g. Poker) with outcomes that can be affected through an external exchange of information between different customers (e.g. a telephone conversation) will not be permitted unless clear rules, compensating controls or technology is put in place to assure the Commission that the prospect of cheating is addressed and minimised.
2. Multi-customer games with outcomes that can be affected through the use of automated end customer devices or ancillary computer systems (e.g. chess) must have warnings in the game rules so that customers can make an informed decision whether or not to participate.
3. The operator must ensure customer fairness, as far as it is possible, in the event of a loss of communication to one or more end customer devices during a multi-customer game.
4. Game rules must cater for situations where the operator loses connectivity with the customer.

Game Artwork (Information Displayed)

This section refers to all forms of graphic 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.

1. The functions of all buttons represented on the website and games must be clearly indicated, preferably on the button itself.
2. Edges of the “hot” area of buttons must be clearly defined in the artwork to

prevent clicking near buttons creating a bet or wager.

Bet Display

1. The bet denomination (and where applicable the tokenisation) of the game must be clearly visible on the game screen, or be able to be easily understood.
2. If a game uses tokens or tokenisation, the number of credits registered for each monetary unit for the current game (e.g. £1.00 buys 10 credits) must be displayed on the game screen.
3. The artwork must either state the maximum bet, the number of credits that can be bet per selected line and the number of possible lines available.

   NOTE: It must be clear to the player what the purpose, function and capability of the game actually is without having to search for it.

Result Display

1. The display of the result or outcome of a game must not be misleading or deceptive to the customer (e.g. must not inappropriately indicate a *nearly won* or *near-miss*).
2. The outcome of each game must be displayed for a reasonable length of time.
3. The nature of all prizes must be clearly indicated. If some prizes are in cash, whilst others are in credits, this must be stated.
4. To the extent that is practicable for the range of games offered, only one method of displaying win amounts should be used on the website to avoid confusion.

Jackpot Requirements

The objective of this requirement is to identify controls that an operator should implement to ensure that game jackpots are operating correctly. As jackpots tend to be prizes awarded outside of a normal game operation, additional controls are needed to ensure that customer jackpot entitlements are transparent and correctly awarded to players.

Partial Jackpot Redirection

1. Diversion Pool schemes, where a portion of the jackpot contribution is redirected to another pool so that when the jackpot is won, the Diversion Pool is added to the seed of the next jackpot. The following requirements apply to such schemes:

   - A jackpot redirection scheme must not have a mathematical expectation of an infinite diversion pool, that is to say, that the percentage that goes to any diversion pool is dealt with correctly in the mathematics of the jackpot.
   - Where a Diversion Pool is used to fund a “minimum or start-up level” the minimum jackpot amount is deemed to be zero for the purposes of calculations of expected customer return; i.e. in calculating customer return the start-up prize can only be counted once.
   - Diversion pools must not be capped.

Multiple Jackpot Winners

1. 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 a resolution of this possibility.

Jackpot Financial Liability

1. The rules of the game must provide for any planned or unplanned termination / discontinuation of a jackpot. Of particular concern is how any outstanding pool amounts are dealt with in order to ensure customer fairness.

Jackpot Shutdown

1. There are instances in this document where it is indicated that the jackpot must be “shutdown”. A jackpot shutdown requires the following action:
    - Clear indication must be given to customers that the jackpot is not operating (e.g. by displaying “Jackpot Closed” on end customer devices).
    - It must not be possible for the jackpot to be won while in the shutdown state.
    - It must not be possible for the customer to contribute to a shutdown jackpot.
    - Activation of the jackpot from the shutdown state must reinstate the jackpot with the identical parameters (including jackpot value, and hidden win amount for mystery jackpots) as before the shutdown.
    - Removal of a Jackpot, which contains funds, for any reason is only to be performed using a process previously approved by the Regulator.

Jackpot records

1. The operator must store and maintain the following records at a minimum:
    - Total amount contributed / won (normally equal) for each previous jackpot, including separate figures for any diverted amounts,
    - Grand total amount contributed / won (normally equal) for all previous jackpots combined,
    - Total amount contributed for current jackpot, including separate figures for any diverted amounts.
    - Reason for the shutdown.

Jackpot Recovery

1. In order to enable the recovery of the current value of the jackpot amount in the case of an operator failure, at least 1 or 2 processes are required:
    - The current value of the jackpot amount must be stored in at least two physically separate devices, or

- The current value of the jackpot amount must be able to be accurately calculated from other available record information that is not stored in the same system as the jackpot amount.

Security Requirements

The objective of this requirement is to identify logical and physical security controls that an operator should implement to ensure that information is protected. This is of particular importance as the operator is so reliant on the integrity of the supporting information systems.

Controls should be implemented that are consistent with up-to-date information security principles in relation to confidentiality, integrity and availability.

General Principles

1. There are many types of threat to electronic gambling systems. The operator should be aware of threats to the hardware, data and customers in their systems caused by failures in their security protocols.
2. With this in mind, operators must put adequate security policies, procedures and mechanisms in place to ensure that:
    - Sensitive customer data remains confidential and is protected from theft and misuse, including:
        - i. Names
        - ii. addresses,
        - iii. credit and debit card details
        - iv. account numbers,
        - v. passwords / PINs
        - vi. The answers to challenge questions.
    - Customer account details are only available to authorised people.
    - The integrity of gambling and account transactions can be assured and that modifications to accounts and gambling transactions can be traced and explained (i.e. audit trails).
    - Customer transactions are not lost through events such as systems failures, or unauthorised modification by entities internal or external to the operator; and
    - The integrity of game outcomes can be relied upon – where events are based on the output of random number generators, the random numbers and the means by which they are used to determine the game outcome, are to be protected from unauthorised modification and can be traced and explained.

Please refer to the **Customer Account Security** section for more information.

Critical Systems

1. Industry “Best Practice” security must be provided for critical systems used by the Operator. This security must take into consideration risks posed by both internal and external threats. The following systems must be adequately protected:
    - Systems that record, store, process, share, transmit or retrieve sensitive customer information, e.g. credit/debit card details, authentication information;
    - Systems that generate, transmit, or process random numbers used to determine the outcome of events;
    - Systems that store the results or state of events;
    - All points of access, either physical or electronic to any and all of the above systems (including other systems that are able to communicate directly with core critical systems); and
    - Communication networks that transmit sensitive customer information.

Detailed Security Requirements

1. Operators must have an up-to-date security policy that is reviewed at least annually, or more regularly if required by the Commission. This review is to be conducted by management staff.
2. Operators must ensure that a suitably qualified third party assesses the security of their systems annually and after any significant changes that are likely to affect the security of systems (e.g. a change of hosting facilities, or new access media). An external penetration test, conducted by a third party, is strongly recommended for systems connected to the Internet.
3. Staff with direct access to critical systems must receive security training appropriate to their role.
4. Critical systems must have adequate physical security.
5. Physical access to systems must be restricted.
6. Equipment used to store sensitive data must have data securely removed before disposal.
7. Equipment holding data backups must be stored securely.
8. Production and test/development facilities must be logically and/or physically separated.
9. Agreements with third parties providing hosting and/or other services to the gambling system must contain a provision for implementation of appropriate security measures.
10. The operator must have policies and procedures for managing third parties and monitoring adherence to security requirements.
11. 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.

12. 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.

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

14. Appropriate network segregation must be implemented.

15. Access to network services must be restricted to those users with specific authorisations and pertinent requirements to access them.

16. 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.

17. 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.

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

19. Faults must be logged, analysed and appropriate action taken.

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

21. Operators must maintain an up-to-date access control policy. Access to critical systems and functionality must be restricted to users on a business need basis.

22. Access to systems must be controlled by a secure log-on procedure.

23. The allocation and use of system privileges must be controlled and restricted.

24. When a member of staff with direct access to critical systems leaves the organisation their access rights must be disabled immediately, and then be removed as soon as possible.

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

26. Applications must implement appropriate data handling methods, including validation of input and rejection of deliberate or unintentional corrupt data.

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

28. Operators must have and implement appropriate policies and procedures for the use of encryption and the management of cryptographic keys.

Security of Data Transmission and Data Storage

1. Where customer account information and / or game play data is either:

   a) being passed over communication lines (e.g. the Internet), or

   b) being stored somewhere within the game servers or supporting servers (e.g. in the database), then such data must be protected (i.e. encrypted) commensurate with the sensitivity of that data. Examples of sensitive data that require encryption include, but are not limited to:

- Customer identity details (including customer identity verification results),
- Credit and debit card details,
- PINs and passwords,
- Account details and balances,
- Customer protection limitations,
- Customer protection exclusions,
- Money transfers to and from customer accounts,
- Changes to account details (e.g. change of address, change of credit card, change of name, etc.), and
- Game play (i.e. games played, amounts bet, amounts won, jackpots won, etc.).

2. 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.

Data Logging Requirements

The objective of this requirement is to identify key events that should be logged and retained by an operator. This will ensure that critical historical information and transactions will be available for review or investigation if required.

General Requirements

1. The operator must be capable of retaining and backing up all recorded information, as discussed herein. Data must be retained for and at a minimum to meet Jersey’s Data Protection Law timescales. Accordingly, among other implications, the number of digits to be used in all fields must therefore be based on appropriately projected performance and business.
2. All time stamping used throughout recorded information must make use of the 24-hour format, with the time zone clearly defined.
3. All date stamping implemented throughout recorded information must make use of a consistent format to be prescribed by the operator.

Customer Account Information

1. For each individual customer account, the operator must maintain and back up the following information and upon request be capable of reporting this information, for a user-specified period of time:
    - Customer identity details (including customer identity verification results),

- Account details and current balance,
- Changes to account details (e.g. change of address, change of credit card, change of name, etc.),
- Any self-imposed customer protection limitations,
- Any self-imposed customer protection exclusions,
- Details of any previous accounts, including reasons for deactivation,
- Deposit / withdraw history, and
- Game play history (i.e. games played, amounts bet, amounts won, jackpots won, etc.).

2. For customer accounts as a whole, the operator must be capable of generating the following reports, for a user-specified period of time, upon request:
    - A list of all active customer accounts,
    - A list of all inactive customer accounts (including reasons for deactivation),
    - A list of all accounts for which the customer has currently (or previously) imposed a customer protection self-exclusion,
    - A list of all accounts for which the customer has currently (or previously) been excluded from the site by the operator (i.e. involuntary exclusion),
    - A list of all accounts for which the customer's funds have currently (or previously) been inactive for a period of time exceeding 90 days,
    - A list of all accounts for which one or more of the customer's deposits and / or withdrawals have exceeded an operator-configurable limit (i.e. large deposits / withdrawals). The limit must be configurable for single transactions, as well as aggregate transactions over a user-defined time period.
    - A list of all accounts for which one or more of the customer's wins have exceeded an operator-configurable limit (i.e. large wins). The limit must be configurable for single wins, as well as aggregate wins over a user-defined time period.

Gambling Session Information

1. For each individual gambling session (i.e. customer login/logout times), the operator must maintain and back up the following information, and be capable of reporting this information upon request:
    - Unique customer ID,
    - Gambling session start and end time,
    - Game play information for sessions (i.e. games played, amounts bet, amounts won, jackpots won, etc).

2. For gambling sessions as a whole, the operator must be capable of generating the following reports upon request:
   - a) A list of all currently active gambling sessions.
   - b) A list of all interrupted sessions.

Game Information

1. For each individual game played, the operator must maintain and back up the following information, and be capable of reporting this information upon request:
   - Unique customer ID,
   - Unique game identifier,
   - Game start time, according to operator,
   - Game end time, according to operator,
   - Customer account balance at start of game,
   - Amount wagered,
   - Contributions to jackpot pools (if any),
   - Current game status (e.g. games in progress, complete, etc…) Please note: the operator must maintain records of any game that fails to complete, and the reason why the game failed to complete)),
   - Game result / outcome,
   - Jackpot wins (if any),
   - Amount won,
   - Customer account balance at end of game.
2. The operator must maintain and back up all information, and be capable of reporting on it, for a user-specified period of time, upon request. A list of all games hosted by the website, including approved game / paytable versions (e.g. “Jacks or Better Video Poker – Game Type XYZ – Paytable Number 123”).

Significant Event Information

The operator must maintain and backup, a log of all significant events on the system, as determined by the Commission.

1. For significant events, the operator must maintain and back up the following information, and be capable of reporting on it upon request, events that include, but are not limited to:
   - Changes made by the operator to game parameters,
   - Changes made by the operator to jackpot parameters,
   - New jackpots created,
   - Jackpot wins, and

- Jackpot shutdowns.
- Switch to Disaster Recovery (DR) systems,
- Irrecoverable loss of customer-related data,
- Significant periods of system unavailability.

2. External computer systems that affect game outcome or win amounts must maintain a log of date and time stamped significant events, if they are not transferred immediately to the operator.
3. The operator must be able to receive and store all significant events from external computer systems that affect game outcome or win amounts.
4. The operator must provide a means to view significant events from external computer systems that affect game outcome or win amounts, including the ability to search for particular event types.

Shut Down and Recovery

The objective of this requirement is to ensure that operators' systems maintain data and game integrity following an unexpected event or planned system shutdown.

1. The operator must be able to perform a graceful shutdown in the event of a simple power failure, and not restart automatically on power up.
2. In the event of a critical hardware / software failure, the operator must be able to recover all critical information from the time of the last backup to the point in time at which the system failure occurred (no time limit is specified).
3. The operator must have disaster recovery capability sufficient to ensure customer entitlements are protected and, that auditability is permissible up to the point of the disaster.
4. The operator must be able to recover from unexpected restarts of its central computers or any of its other components.
5. The operator hardware platform and operating system must be proven to be reliable.
6. The operator must have a mechanism whereby all gambling offered on the operating system can be disabled, as a whole, by the operator – with full consideration to the associated requirements listed above.

Anti-Money Laundering Requirements

The objective of this requirement is to identify controls that an operator should implement to minimise the potential for money laundering activities. This includes methods for detecting potential money laundering and reporting suspicious activity to the appropriate bodies.

General Anti-Money Laundering Controls

In support of anti-money laundering efforts world-wide, the operator must ensure that documented technical procedures and policies are put in place in order to satisfy the following objectives:

- That it is possible to effect account closures in order to halt suspected money-laundering,
- That it is possible to impose general or risk-based deposit limits on customers in order to reduce the overall exposure to money-laundering. Such limits should not be invoked in response to suspected money-laundering activity in order to avoid alerting the suspect to a potential investigation.
- That customer accounts be monitored for opening and closing in short time frames,
- That customer accounts be monitored for deposits and withdrawals without associated game play,
- That cheques and Electronic Fund Transfers (EFTs) be reviewed and returned to customers marked “Account Closure” or “Over-contribution”, and be identified separately from a win,
- That all suspicious transactions be reported to the appropriate body in compliance with Money Laundering regulations implemented within the jurisdiction.

1. Payments from a customer’s account must be paid directly to an account with a financial institution in the registered name of the customer, or made payable to the customer and forwarded to the customer’s registered address.
2. A customer must not be permitted to deposit from one account with a financial institution and subsequently withdraw to a different account.
3. A customer must not be permitted to move money into another customer’s account, except as permitted in the rules of peer-to-peer gambling.
4. Where the customer’s account is to be closed any money left in the account must be remitted to the customer using the registered name and address except in case of an ongoing criminal investigation.
5. All changes made to customers contact details must be recorded, including the old (replaced) details, and retained for a period stipulated by the anti-money laundering regulations.
6. A responsible staff member will be appointed Money Laundering Reporting Officer (MLRO), and will be responsible for all areas of anti-money laundering by the operator.
7. The operator must be aware of Jersey’s anti-money laundering legislation (i.e. the “Handbook for The Prevention and Detection of Money Laundering and the Financing of Terrorism”, which can be downloaded from the Jersey Financial Services website).
8. Appendix A of this document outlines in further detail the areas of AML/CFT that the JGC will focus on during both the application process and it’s post licencing regulatory activity i.e. audit and inspection.

Software Testing, Maintenance and Approval

The objective of this requirement is to identify controls that an operator should implement to control the software development, user acceptance testing (UAT), and certification life-cycle.

1. The operator must have the software tested by a testing house certified by the Commission prior to the software being deployed to a live environment.
2. For new or modified systems, RNGs or games, the source code shall be commented on in an informative and useful manner and able to be compiled. The following source code information should be made available.
    - File / module / function name(s);
    - Brief description of file / module / function purpose(s); and
    - Edit History, including who modified it, when and why.
3. 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:
        - Customer Account Registration;
        - Customer Account Login (Username & Password);
        - Customer Interface to Customer Account;
        - Operator Interface to Customer Account;
        - Operator Accounting and Financial Reporting Capabilities;
        - Customer Protection / Exclusion Systems;
        - Operator Payment Systems & Financial Institution Interfacing;
        - Customer Location & Identity Verification Software; and
        - Customer Account Deactivation.
4. For the games that run on the base system the following documentation must be available:
    - Game name;
    - Game version number(s);
    - Paytable version number(s);
    - Detailed game rules, including all options and bonus features;
    - Detailed breakdown of all paytables, payouts and mapped symbols present in the game; and

- A formal mathematical treatise of the derivation of the theoretical Percentage Return to Customer (%RTP) of the game.

5. For RNGs 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.

Appendix A - Guideline to the Post Licencing Regulatory Framework

The licence or permit may be valid for 5 years, renewable annually on the anniversary of the licence / permit.

Governing Legislation

Gambling (Jersey) Law 2012

All remote gambling licences are subject to the Gambling (Jersey) Law 2012. Remote gambling permits are subject to this Law and also requirements of the Gambling (Ancillary and Miscellaneous Provisions) (Jersey) Regulations 2012.

Risk Based Approach

The Commission uses a risk based approach to regulation and some areas, like player registration and validation are considered high risk compared to the employee due diligence which is generally considered medium risk.

The Commission uses an inspection check-list and breaks its inspections into the following areas:

- Risk Based Approach
    - Individual responsible, qualifications and training
    - Risk approach approved by the board
    - Procedures reflect the risk based approach
    - Risk based approach schedule, how often is it reviewed.
    - How are risks measured against clients
- Corporate Governance
    - Internal Procedures and Controls
        - Software systems
        - Internal procedures and controls documentation freely available to all staff members
        - Systems backups, schedules
        - Disaster recovery plan, schedule
        - Number of system administrators
        - Holiday cover
    - Financial Systems

        - Software used, patches, updates, routine maintenances
        - Staff qualifications and training
        - Players funds, segregation, operating funds – How
        - Audits, financial year, auditors, any changes since application/grant of licence
        - Holiday cover
    - MLRO
        - Individual responsible, qualifications and training
        - JFSC and JGC – current named officer
        - MLRO Duties and staffing
        - Deputy MLRO
        - Holiday cover
    - Outsourced functions
        - What functions are outsourced, to whom and why
    - Declaration of conflict of interests, Board or otherwise
        - Are there any

- Customer Verification/Authentication
    - Age verification – how is it done, software, any manual intervention – if so what.
    - How often is the customer reviewed and what is reviewed and how.
    - Due diligence on the customer, worldcheck, internet searches
    - Are high risk clients identified i.e. Politically Exposed Persons, if so, how are these clients dealt with. What controls are in place
        - How many have been identified
        - From which jurisdictions
        - What business aspects are the PEPs involved with
        - Validation/verification on the source of funds

        - Ceasing/refusing relationship with a PEP, how and in what circumstances

        - Accept cash deposits or funds transferred to third parties

        - How are high risk clients identified in the internal controls and procedures

    - Verification and validation on the source of funds

    - What procedures are in place to ensure client due diligence is done prior to client acceptance

    - Client verification failure, how is this dealt and how is the relationship terminated

- Transaction Monitoring and Recording

    - How long are players records kept

    - How long is player play data kept

    - Are these backed up

    - Is there a disaster recovery solution

    - How often is the backup data verified and tested for integrity

- AML Suspicion Reporting – Suspicion Transaction Reports

    - Reporting forms and format

    - Staff training on reporting to the MLRO

    - Record Keeping, how long are these kept

    - How many reports have been reported to the MLRO

    - How many reports have been reported to the JFSC

- Employee Due Diligence and Training

    - Staff PNCs, which staff are subject to it, which not and explain

    - Staff references, are these followed

    - Staff induction programme

    - Staff handbook and Jersey employment contracts

    - Staff training schedule, to include AML reporting and procedures

- Outsourced training, if so to whom and why.

The above checklist is by no means final and will evolve over time and adapt to new JFSC /JGC requirements and technology advancements.

The Law and Regulations allow for the Commission to make copies of any data, paper copies of any documentation that it sees fit and that may assist with any investigation.

Databases

The Commission currently takes the view that as gaming databases have millions of records it would not ordinarily seek to look into these as matter of course. If, however, there was a suspicion of irregularity or other just cause, it may resort to data mapping of the game databases or other methodologies necessary to investigate any such instances.

Databases are not required to be verified or tested by any third party testing house, but should be declared so the Commission is aware of whether the system is a commercial database server or an Open Source database, i.e. mysql.

Application Servers (Hardware and Software)

The Commission would ordinarily seek to ascertain during inspection that these actually existed as per the application. This does not apply if the operator is using a cloud solution from the accredited hosting provider.

Any changes to critical hardware/software or Cloud solution service, must be reported to the Commission and these are checked during inspection against our records.

Games

All games are required to be individually tested by an accredited independent testing lab, and during any inspection, the game versions and hashing algorithms are checked and tested against the certificate held on file by the Commission.

Document History Log

Date	Change Description
28th October 2011	Initial release
12th December 2011	Adopted
25th September 2015	Revised
31st July 2019	Revised

Jersey Gambling Commission

4th Floor Osprey House 5-7 Old Street
St. Helier, Jersey, JE2 3RG

Tel: +44 (0)1534 828 540

Email: info@jgc.je

Web: http://www.jgc.je