New section/objective added
New control added
Modified control (modifications underlined)

Annex A

G.6	Business continuity management	
G.6.2	**Business continuity plan and exercises**	
Objective:	To ensure the protection of organization personal and infrastructure in case of violent situations targeting the organization.	
G.6.2.1	Business continuity plan	*Control* Continuity exercises shall be planned, performed and evaluated in regular intervals to prepare the organization on crisis situation
G.6.2.2	Violent situations	*Control* Physically security measures to prevent damage of terror attacks or other threats shall be panned to protect personal and business processes

Annex B

L.2.4	**Electronic Lottery Draws**	
Objective:	To ensure electronic drawing system integrity by physical and logical protection	
L.2.4.1	Physical and logical protection of the technical system	*Control* Measures shall be taken in order to ensure only those authorized have physical access to, and logical protection of, both the Random Number Generator (entropy source) and the drawing algorithm in order to prevent any modification of the algorithm and the entropy source settings. The physical system(s) must be protected against theft, unauthorized modifications, and interference.
L.2.4.2	Secured transmissions	*Control* Measures shall be taken in order to ensure integrity and authenticity of the data transmitted between the RNG (entropy source) and the drawing algorithm
L.2.4.3	Electronic draw randomness and integrity verification	*Control* Before deployment, tests and verifications shall be performed by independent parties in order to verify that the electronic drawing system is random. The organization shall document its policy related to after-deployment tests and verifications in order to verify that the random number generator and drawing algorithm is performing as specified.
L.2.4.4	Separation of duties	*Control* A specific procedure shall be implemented concerning separation of duties involved in an electronic draw in order to prevent any internal fraud. Notably no one person should be allowed to perform more than one of the following types of duties; maintaining, monitoring or performing draws on electronic gaming equipment.

New section/objective added
New control added
Modified control (modifications underlined)

L.6	Digital sales channels and interactive services	
L.6.1	**Digital gaming systems**	
Objective:	To protect the confidentiality, integrity and availability of digital gaming systems in order to protect gaming and player data.	
L.6.1.1	Layered systems architecture	*Control* The organization shall provide a layered approach to security within the digital gaming systems architecture to ensure secure storage and processing of data
L.6.1.2	Active and passive attacks	*Control* Appropriate measures shall be in place to detect, prevent, mitigate and respond to common active and passive technical attacks. The organization shall have established procedure to gather cyber threat intelligence and act on it appropriately. The organisation shall also have agreed patching policies for digital gaming systems, whether developed and supported in house or by a third party.
L.6.1.3	Network segregation	*Control* Production databases containing player or transaction data shall reside on networks separated from the servers hosting the web pages.
L.6.1.4	Session information	*Control* The user session information shall always be created randomly, in memory and shall be removed after the user's session has ended
L.6.1.5	Identify points of ingress and egress	*Control* All entry and exit points to open public network systems shall be identified, managed, monitored and controlled. The organization shall monitor all its digital gaming systems in order to prevent, detect, mitigate and respond to cyber-attacks.
L.6.1.6	Generation and storage of logs	Logs shall be generated on each sensible system component in order to monitor and rectify anomalies, flaws and alerts. All logs shall be stored in order to be presented as evidence in the jurisdiction the lottery operates.
L.6.1.7	Security testing	There shall be appropriate security testing on major system changes. Regular intrusion testing that attempts to identify and exploit vulnerabilities or other system weaknesses shall be performed.

L.6.2	**Player account**	
Objective:	To protect the player and to fight fraud and money laundering.	
L.6.2.1	Player identification and data protection	*Control* There shall be a formal process for identification of player. Both player data and the wallet shall be considered as critical assets for the purposes of risk assessment
L.6.2.2	Multiple player accounts	*Control* There shall be an established procedure for the use of multiple player accounts whenever this does not exist only one account per player shall be allowed.

New section/objective added
New control added
Modified control (modifications underlined)

L.6.2.3	Players exclusion	*Control* There shall be an established process for excluding players in accordance with local applicable laws and/or internal procedures
L.6.2.4	Multiple payment instrument holder	*Control* There shall be an established procedure for assuring the match of ownership between the payment type holder and the payer account holder

L.6.3	**Game design and approval**	
Objective:	To ensure that the game design meets legal and regulatory requirements and are authorized at the appropriate level before going live.	
L.6.3.1	Documented xxxxx game procedures	*Control* Established rules shall cover design and development. In addition, game rules shall be accessible by players.
L.6.3.2	Game approval and modification	*Control* An approval procedure shall be defined to validate that every new game and relevant modifications on the digital are controlled. Final game design shall be formally approved through a process involving the Security Function.

L.6.4	**Securing payment methods**	
Objective:	To protect payments methods against fraudulent uses	
L.6.4.1	Data collection	*Control* Collection of sensitive data directly related to payment shall be limited to only the data strictly needed for transaction
L.6.4.2	Payment method protection	*Control* Adequate measures shall be taken in order to protect any type of payment used in the system from a fraudulent use
L.6.4.3	Payment service approval	*Control* The organization shall verify that the payment service ensures the protection of the player data, including any personally identifiable information given by the player or payment related data
L.6.4.4	Transactional records related to payments	*Control* The organization shall generate all transactional records of players account. The data recorded shall allow the organization to trace a single financial activity of a player from another.

New section/objective added
New control added
Modified control (modifications underlined)

L.7	**Sports betting**	
L.7.1	**Selecting the offer**	
Objective:	To ensure integrity of the betting offer.	
L.7.1.3	Authorized betting options list	*Control* Maintain a list of betting types per game type. Specific procedures shall be implemented in the case of nonprofessional events.
L.7.2	**Events and Odds management**	
Objective:	To assure the integrity of events and their corresponding odds.	
L.7.2.1	Selection of events	*Control* A procedure to select events based on the authorized events list shall be established to assure the integrity of the offering.
L.7.2.2	Setting and updating the odds	*Control* There shall be established procedures for setting and updating the odds and/or blocking events, taking into account market forces. A process shall exist for validating accuracy and preventing fraudulent activities. The procedures shall be based on respect of integrity, responsible gaming, and ensuring transparency.
L.7.2.3	Setting of the betting margin	*Control* Authorized levels for the margin of each bet type shall be documented and approved.
L.7.2.4	Safeguarding payout levels	*Control* The organization shall establish a set of measures to ensure authorized payout levels are not exceeded.
L.7.3	**Resulting handling**	
Objective:	To ensure reliance on reliable results.	
L.7.3.1	Results for completed events	*Control* There shall be a policy for the confirmation of results based on qualified and approved sources, before publicly announcing results and declaring winners.
L.7.3.2	Results records	A backup record of all results shall be kept and identified as a critical asset.
L.7.4	**Monitoring for fraud and money laundering**	
Objective:	To ensure actions to minimize the risk of fraud and/or money laundering.	
L.7.4.3	Customer transaction monitoring	*Control* There shall be procedures in place to detect betting irregularities, including regional patterns. In case of detection a process shall be in place to notify the regulatory authority and if necessary the relevant sport governing body.

New section/objective added
New control added
Modified control (modifications underlined)

L.7.4.4	Cash payment of winnings	*Control* A procedure shall be established specifying thresholds of payment and methods of collection
L.7.4.5	Winners monitoring	*Control* Subject to applicable laws, a procedure shall be established to monitor winners over a certain amount of gains.
L.7.4.6	Deposit monitoring	*Control* Establish a level above which deposits of a certain size are monitored.
L.7.5	**Live betting**	
Objective:	To ensure the propriety of the offering of bets during game time.	
L.7.5.3	Courtsiding prevention mechanisms	*Control* Ensure customer protection and fraud/integrity protection through the provision of a safety mechanism to account for delay in live pictures.
L.7.6	**Duties separation and internal control**	
Objective:	To avoid internal collusions	
L.7.6.1	Duties separation	*Control* There shall be a separation of duties to ensure that no group has overall control without oversight.
L.7.6.2	Corporate betting policy	*Control* There shall be an internal policy addressing employees' rights to play.

New section/objective added
New control added
Modified control (modifications underlined)

L.8 Interactive Video Lottery Terminals (VLT)

L.8.1 Video Lottery Terminals (VLT)

Objective: To ensure secure operation of VLT terminals no matter system design or operating models.

L.8.1.1	VLT terminals	Control VLT terminals shall be monitored concerning security and prize pay-out percentage.
L. 8.1.2	VLT games	Control The game-rules and overall prize-payout percentage shall be available for the customer
L.8.1.3	VLT game certificate	Control Dedicated games for VLT shall be tested and a certificate to provide evidence of integrity has to be maintained/issued
L.8.1.4	VLT incidents	Control There shall be documented procedures to handle dispute or protest from customer regarding a win or loss