A code of conduct shall be issued to all personnel when initially employed. All personnel shall formally acknowledge acceptance of this code.

The security function shall report to no lower than executive level management and shall be independent of the technology function with regard to the management of security risk.

The head of the security function shall be a full member of the security forum and be responsible for recommending security policies and changes.

A code of conduct shall be issued to all personnel when initially employed. All personnel shall formally acknowledge acceptance of this code.

The security function shall be responsible for developing a security strategy in accordance with the overall business. The security function will subsequently work with the other business units to implement the associated action plans. It shall be involved in reviewing all tasks and processes that are necessary from the security perspective for the organization, including, but not limited to, the protection of information and data, communications, physical, virtual, personnel, and overall business operational security.

A security forum or other organizational structure comprised of senior managers shall be formally established to monitor and review the ISMS to ensure its continuing suitability, adequacy and effectiveness, maintain formal minutes of meetings, and convene at least every six months.

A security function shall exist that will be responsible to draft and implement security strategies and action plans. It shall be involved in and review all processes regarding security aspects of the organization, including, but not be limited to, the protection of information, communications, physical infrastructure, and game processes.

A security forum or other organizational structure comprised of senior managers shall be formally established to monitor and review the ISMS to ensure its continuing suitability, adequacy and effectiveness, maintain formal minutes of meetings, and convene at least every six months.

The security function shall report to no lower than executive level management and shall be independent of the technology function with regard to the management of security risk.

The head of the security function shall be a full member of the security forum and be responsible for recommending security policies and changes.
<table>
<thead>
<tr>
<th>Clause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.2.1.7 Segregation of duties</td>
<td>There shall be a policy to implement segregation of duties detailing the respective roles and responsibilities of the people in charge of critical processes that could impact the integrity of a game, such as, but not limited to, draw processing and prize payment. The intention is to avoid possible collusion. Furthermore no single group or team shall have overall control in a way that could impact game integrity without management oversight. In the context of a lottery technology supplier, this control shall relate to critical areas of code that could impact the integrity of a game such as, but not limited to, handling the input-to-output from random number generation used for determining the outcome of games.</td>
</tr>
<tr>
<td>CONSOLIDATED</td>
<td>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. There shall be a separation of duties to ensure that no group has overall control without oversight.</td>
</tr>
<tr>
<td>G.2.2 Staff protection</td>
<td>Objective: To ensure that the staff are receiving an adequate level of protection.</td>
</tr>
<tr>
<td>G.2.2.1 Policy on staff protection</td>
<td>A policy shall be established to ensure that staff conducting lone working, those working remotely outside lottery premises, or those working inside lottery premises in areas with public access, are receiving an adequate level of protection with regard to both their safety and security.</td>
</tr>
<tr>
<td>CONSOLIDATED</td>
<td>Physical security measures to prevent damage of terror attacks or other threats shall be planned to protect personnel and business processes.</td>
</tr>
<tr>
<td>G.3 Physical and environmental security</td>
<td>Objective: To ensure that access to production gaming data centers or other systems areas important for the gaming operations are adequately secured.</td>
</tr>
<tr>
<td>G.3.1.1 Physical entry controls</td>
<td>Physical access to production gaming system data centers, computer rooms, network operations centers, and other defined critical areas, shall be restricted and adequately secured or monitored by staff at all times. While this control is risk based, in practice it shall require a minimum of an auditable two-factor authentication process.</td>
</tr>
<tr>
<td>MODIFIED</td>
<td>Physical access to production gaming system data centers, computer rooms, network operations centers and other defined critical areas shall have a two-factor authentication process. Single-factor electronic access control methods are acceptable if the area is staffed at all times.</td>
</tr>
<tr>
<td>G.4 Access control to gaming systems</td>
<td>Objective: To ensure authorized user access and to prevent unauthorized access to gaming systems. For technology suppliers G.4 controls shall be applied to the code repositories used to develop gaming systems.</td>
</tr>
<tr>
<td>G.4.1.1 User access functions</td>
<td>The range of functions available to the user shall be defined in conjunction with the process owner, the IT function, and the security function.</td>
</tr>
<tr>
<td>MODIFIED</td>
<td>The range of functions available to the user shall be defined in conjunction with the process owner, the IT function and the security function.</td>
</tr>
<tr>
<td>G.4.1.2 User access logging</td>
<td>All actions performed on the gaming systems by human or system accounts shall be logged and these logs shall be monitored, regularly reviewed, and acted upon as appropriate.</td>
</tr>
<tr>
<td>MODIFIED</td>
<td>All actions performed through remote user access shall be logged and these logs shall be regularly reviewed.</td>
</tr>
<tr>
<td>G.5 Information systems maintenance</td>
<td>Objective: To protect the confidentiality, authenticity, and integrity of cryptographic keys and important gaming, lottery, and customer related information by cryptographic means.</td>
</tr>
<tr>
<td>G.5.1.1 Cryptographic controls for the confidentiality and integrity of data at rest on portable systems and on lottery terminals</td>
<td>Cryptography to protect the confidentiality of information shall be applied for sensitive information on portable computer systems (e.g. laptops, removable media such as USB devices, and similar) and to protect the integrity of sensitive information held at rest on lottery terminals.</td>
</tr>
<tr>
<td>MODIFIED</td>
<td>Encryption shall be applied for non-public organization data on portable computer systems (laptops, USB devices, etc.).</td>
</tr>
<tr>
<td>G.5.1.2 Cryptographic controls for the confidentiality and integrity of data in transit over networks</td>
<td>Cryptography to protect the confidentiality and integrity of information as appropriate shall be applied for sensitive information passed over networks, which risk analysis has shown to have an inadequate level of protection. This includes, but is not limited to, validation or other important gaming information, customer data, and financial transactions.</td>
</tr>
<tr>
<td>MODIFIED</td>
<td>Encryption shall be applied for sensitive information passed over networks, which risk analysis has shown to have an inadequate level of protection, including validation or other important gaming information, electronic mail, etc.</td>
</tr>
<tr>
<td>G.5.1.3 Cryptographic controls for the integrity of sensitive ticket data</td>
<td>Cryptographic controls for integrity shall be applied for the storage of winning ticket data and validation information. This control applies to all game types.</td>
</tr>
<tr>
<td>MODIFIED</td>
<td>Integrity measures shall be applied for the storage of winning information ticket data and validation information.</td>
</tr>
<tr>
<td>G.5.2 System testing</td>
<td>Objective: To enable and conduct system testing.</td>
</tr>
<tr>
<td>G.5.2.1 Test methodology policy and data</td>
<td>The test methodology policy shall include provisions to prevent the use of data created in a live production system for the current draw period and to prevent the use of player, retailer, or staff personal information. In this context current draw period shall be defined as the period for which prizes can still be claimed.</td>
</tr>
<tr>
<td>MODIFIED</td>
<td>The test methodology policy shall include provisions to prevent the use of data created in a live production system for the current draw period and to prevent the use of player personal information.</td>
</tr>
<tr>
<td>G.5.2.2 Gaming system security testing</td>
<td>Thorough testing of the gaming system security functionality shall be performed prior to production environment use and on any significant changes.</td>
</tr>
<tr>
<td>NEW</td>
<td>Thorough testing of the gaming system security functionality shall be performed prior to production environment use and on any significant changes.</td>
</tr>
</tbody>
</table>
### G.5 Information systems maintenance

#### G.5.3 Cloud security

**Objective:** To ensure information security of lottery systems hosted in the cloud.

<table>
<thead>
<tr>
<th>Clause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.5.3.1</td>
<td>Cloud security: Cloud environments that host gaming systems shall be compliant with ISO/IEC 27017. A cloud environment is defined as an off-site, third-party platform with a suite of applications that the organization subscribes to for services such as: Infrastructure as a Service; Platform as a Service; Software as a Service; etc.; that are required to operate its business. For technology suppliers the WLA-SCS G.5.3 controls shall be applied to the code repositories used to develop gaming systems.</td>
</tr>
</tbody>
</table>

### G.6 Availability of services and business continuity

**Objective:** To ensure the protection of the organization’s image and reputation and to counteract interruptions to business activities.

<table>
<thead>
<tr>
<th>Clause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.6.1.1 Availability and resilience requirements</td>
<td>The organization shall have documented the list of critical services to players (both retail and digital channels) that are required for the continued operation of lottery games, as well as the availability and resilience requirements of those services. Systems shall be architected to meet those requirements.</td>
</tr>
<tr>
<td>G.6.1.2 Business Continuity</td>
<td>The organization shall prepare a documented business continuity plan that covers, at minimum, the continued operation of lottery games and continued stakeholder confidence in the integrity of lottery operations. The organization shall furthermore plan, perform, and evaluate business continuity exercises in regular intervals to prepare the organization for crisis situations, covering the elements included in the business continuity plan.</td>
</tr>
</tbody>
</table>
### Physical Instant Tickets

**L1**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>L.1.1.1</td>
<td>Printer/Ssupplier selection</td>
<td>There shall be a formal approval process that involves the security function.</td>
<td>CONSOLIDATED</td>
<td>L.1.1.2</td>
<td>Final game design shall be formally approved through a process involving the security function.</td>
</tr>
<tr>
<td>L.1.1.2</td>
<td>Integrity requirements and testing</td>
<td>The organization shall implement a documented procedure that covers the entire game lifecycle, from design to destruction, by specifying the integrity requirements for each instant game. The integrity requirements shall include at least, but not be limited to, the following: final visuals and net, price structure, print quality, data entry security, number of tickets, and effective testing of the requirements before the game is accepted.</td>
<td>CONSOLIDATED</td>
<td>L.1.1.1</td>
<td>Formal procedures shall be established covering the design, development, production, and release of instant games.</td>
</tr>
<tr>
<td>L.1.1.3</td>
<td>Game data integrity</td>
<td>There shall be controls to ensure the integrity of game data, including but not limited to the importing of game data into the gaming system and the transfer of validation data between the supplier/operator/retailer.</td>
<td>MODIFIED</td>
<td>L.1.1.4</td>
<td>Specific security requirements relating to the game and the physical instant ticket shall be documented and formally included as part of the contract with the supplier/printer.</td>
</tr>
<tr>
<td>L.1.1.4</td>
<td>Ticket prize confidentiality</td>
<td>Controls shall be in place to ensure that prior to the claiming of a prize no one in the organization has access to the knowledge of whether ticket is a winning ticket and which is not; nor shall they be able to identify the location of the winning ticket and which retailer it has been assigned to.</td>
<td>NOT CHANGED</td>
<td>L.1.1.5</td>
<td>A policy shall be established describing the required audits and laboratory testing of game design and ticket printing.</td>
</tr>
</tbody>
</table>

### Lottery Draws

**L2**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>L.2.1.1</td>
<td>Draw event</td>
<td>A policy shall be established to ensure that lottery draws are conducted as a planned and controlled event and in accordance with a clear working instruction.</td>
<td>NOT CHANGED</td>
<td>L.2.1.2</td>
<td>The organization shall publish a working instruction prior to any draw including special instructions with respect to the draw.</td>
</tr>
<tr>
<td>L.2.1.2</td>
<td>Draw working instructions</td>
<td>The working instruction shall include the composition of a draw team including their contact telephone numbers.</td>
<td>NOT CHANGED</td>
<td>L.2.1.3</td>
<td>The working instruction shall include the duties of the identified members of the draw team.</td>
</tr>
<tr>
<td>L.2.1.3</td>
<td>Draw team members</td>
<td>There shall be controls to ensure the integrity of game data, including but not limited to the importing of game data into the gaming system and the transfer of validation data between the supplier/operator/retailer.</td>
<td>NOT CHANGED</td>
<td>L.2.1.4</td>
<td>The working instruction shall include details of any requirement under the lottery rules for independent observers to be present during a draw.</td>
</tr>
<tr>
<td>L.2.1.4</td>
<td>Draw observers</td>
<td>The working instruction shall include details of any requirement under the lottery rules for independent observers to be present during a draw.</td>
<td>NOT CHANGED</td>
<td>L.2.1.5</td>
<td>The working instruction shall include details of any requirement under the lottery rules for independent observers to be present during a draw.</td>
</tr>
</tbody>
</table>

### Lottery Draw Management

**L.2.1.1**

Objective: To ensure that draws are conducted at times required by regulation and in accordance with the rules of the applicable lottery game.

- **L.2.1.1.1** Draw event
  - A policy shall be established to ensure that lottery draws are conducted as a planned and controlled event and in accordance with a clear working instruction.

### Lottery Draw Operations

**L.2.2**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>L.2.2.1</td>
<td>Draw procedure</td>
<td>The organization shall establish a detailed draw procedure to ensure that all draw functions are conducted in compliance with the rules of the applicable lottery game and regulatory requirements.</td>
<td>NOT CHANGED</td>
<td>L.2.2.1</td>
<td>The organization shall establish a detailed draw procedure to ensure that all draw functions are conducted in compliance with the rules of the applicable lottery game and regulatory requirements.</td>
</tr>
<tr>
<td>L.2.2.2</td>
<td>Draw step-by-step guide</td>
<td>The draw procedure shall include a step-by-step guide of the draw process.</td>
<td>NOT CHANGED</td>
<td>L.2.2.2</td>
<td>The draw procedure shall include a step-by-step guide of the draw process.</td>
</tr>
<tr>
<td>L.2.2.3</td>
<td>Draw location</td>
<td>The draw procedure shall include the definition of the draw location.</td>
<td>NOT CHANGED</td>
<td>L.2.2.3</td>
<td>The draw procedure shall include the definition of the draw location.</td>
</tr>
<tr>
<td>L.2.2.4</td>
<td>Draw attendance and responsibilities</td>
<td>The draw procedure shall include a definition of the attendance at the draw and the responsibilities and actions of all participants.</td>
<td>NOT CHANGED</td>
<td>L.2.2.4</td>
<td>The draw procedure shall include a definition of the attendance at the draw and the responsibilities and actions of all participants.</td>
</tr>
<tr>
<td>L.2.2.5</td>
<td>Draw supervision</td>
<td>The draw procedure shall define the policy regarding the attendance of an (independent) compliance officer or an auditor.</td>
<td>NOT CHANGED</td>
<td>L.2.2.5</td>
<td>The draw procedure shall define the policy regarding the attendance of an (independent) compliance officer or an auditor.</td>
</tr>
<tr>
<td>L.2.2.6</td>
<td>Draw operation security</td>
<td>The draw procedure shall include adequate security measures for the draw operation and all equipment used during the draw process.</td>
<td>NOT CHANGED</td>
<td>L.2.2.6</td>
<td>The draw procedure shall include adequate security measures for the draw operation and all equipment used during the draw process.</td>
</tr>
<tr>
<td>L.2.2.7</td>
<td>Draw emergency</td>
<td>The draw procedure shall include actions in the event of an emergency occurring at any time during the course of the draw.</td>
<td>NOT CHANGED</td>
<td>L.2.2.7</td>
<td>The draw procedure shall include actions in the event of an emergency occurring at any time during the course of the draw.</td>
</tr>
<tr>
<td>L.2.2.8</td>
<td>Draw integrity, alerting and reporting</td>
<td>The lottery shall put a system or process in place to ensure that no individual or individuals with access to the Central Gaming System can manipulate the transactions within, prior to, or post draw, and that a clear audit trail tracking of the user access and transaction audit is established.</td>
<td>NEW</td>
<td>L.2.2.8</td>
<td>A policy shall be established describing the required audits and laboratory testing of game design and ticket printing.</td>
</tr>
</tbody>
</table>

### Lottery Draw Audits

**L.2.3**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>L.2.3.1</td>
<td>Inspection procedure</td>
<td>A procedure for the inspection of draw appliances and ball sets on delivery and thereafter in consultation with an independent authority (to ensure compliance with technical specifications and standards) on a regular basis shall be established.</td>
<td>NOT CHANGED</td>
<td>L.2.3.1</td>
<td>A procedure for the inspection of draw appliances and ball sets on delivery and thereafter in consultation with an independent authority (to ensure compliance with technical specifications and standards) on a regular basis shall be established.</td>
</tr>
<tr>
<td>L.2.3.2</td>
<td>Regular inspection and maintenance</td>
<td>Inspections and maintenance of the draw appliances shall be carried out and documented at least annually to retain the specified standards throughout the machine’s working life.</td>
<td>NOT CHANGED</td>
<td>L.2.3.2</td>
<td>Inspections and maintenance of the draw appliances shall be carried out and documented at least annually to retain the specified standards throughout the machine’s working life.</td>
</tr>
</tbody>
</table>
L.2.3.3 Compatible ball sets  
The organization shall establish a procedure that provides for the use of ball sets manufactured to those measurements and weight tolerances compatible with the drawing machine to be used.  

L.2.3.4 Replacement draw appliance  
The organization shall establish a procedure that provides for the availability of a substitute draw appliance and ball set(s) for use in the event of mechanical problems or failure of any kind, if drawings are broadcast live.  

L.2.3.5 Draw appliance and ball set handling, storage and movement  
The organization shall establish a procedure that provides for the secure storage, movement, and handling of draw appliances and ball sets.  

L.2.3.6 Broadcast/streaming of the draw  
When the draw is broadcast or live streamed over the Internet, there shall be a procedure in place that minimizes the risks associated with data corruption, time delays to the audio and/or video, or changes in graphic generation or display resulting in the public perception that there is an issue with the draw integrity.  

L.2.4 Electronic lottery draw and instant games  
Objective: To ensure electronic drawing system integrity by physical and logical protection. L.2.4 covers both electronic draw based games and electronic instant win games.  

L.2.4.1 Physical and logical protection of the technical system  
Measures shall be taken in order to ensure that only those authorized have physical access to, and logical protection of, both the Random Number Generator (RNG) (entropy source) and the drawing algorithm in order to prevent any modification of the algorithm and the entropy source settings. The physical system(s) shall be protected against theft, unauthorized modifications, and interference.  

L.2.4.2 Secured transmissions  
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  
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 Segregation of duties  
In addition to the control G.2.1.7, a specific procedure shall be implemented for the segregation of duties involved in an electronic draw in order to prevent internal fraud. Notably, no one person shall be allowed to perform more than one of the following types of duties: maintaining, monitoring, or performing draws on electronic gaming equipment.  

L.3 Retailer security  
Objective: To ensure retailer operations, whether on or off-line, conform to the organization’s security requirements.  

L.3.1 Retailer operations  
Objective: To ensure that retailer operations, whether on or off-line, conform to the organization’s security requirements.  

L.3.1.1 Retailer security  
To ensure retailers meet the organizational security requirements, the organization shall specify the obligations of a retailer and the security environment the retailer is required to operate in within an agreed contract.  

L.3.2 Gaming terminal security  
Objective: To ensure the adequacy of the gaming terminal security.  

L.3.2.1 Transaction security  
The data traffic between the gaming terminals and the central gaming system shall be protected and measures to ensure the integrity of the transactions shall be implemented. Where a retailer point of sale device is used instead of a dedicated lottery terminal, the data traffic from the lottery application on the point of sale device to the central gaming system must be protected and not reliant on the security of the retailer point of sale device for the integrity of lottery games.  

L.4 Price payment  
Objective: To ensure that the organization has the necessary controls in place for validation and payment of prizes and to prevent fraud related to unclaimed prizes.  

L.4.1 Validation process  
The organization shall define and implement procedures to ensure the validity of winning transactions, claims and/or tickets for different prize levels and types of games, and process prize payouts therefrom.  

L.4.1.1 Validation process  
The organization shall implement procedures to ensure the validity of winning transactions, claims and/or tickets for different prize levels and types of games.  

L.4.1.2 Unclaimable prize reference  
Each ticket for each game shall have a unique reference number.  

L.4.1.3 Security of unclaimed prize data  
The organization shall implement technical and procedural controls to ensure the confidentiality, integrity, and availability of unclaimed prize data. This includes as a minimum, but is not limited to, access controls on specific transactions yet to be claimed and any validation files. Specific consideration shall be given to access control to restrict access to the data, monitoring of user interaction with the data, and a process for dealing with unauthorized access to or export of the data.  

L.4.1.4 Prize payout procedure  
There shall be a prize payout procedure that defines a maximum prize claim period; includes a process to audit final transfers upon game settlement; details the rules and due diligence required prior to making a decision on payout for a lost, stolen or damaged ticket; details the procedure with regard to requiring evidence of entitlement, and accounting for prize payments.
The organization shall provide a layered approach to security within the digital gaming systems architecture to ensure secure storage and processing of data. Production databases containing player or transaction data shall reside on networks separated from those used by interactive services. 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.

L5.6.2.1 Player account
Objective: To protect the player and to manage the risk of fraud and money laundering.

L5.2.1 Player account
There shall be a formal process for identification, authentication and authorization of a player. Both player data and the wallet shall be considered as critical assets for the purposes of risk assessment. The procedure shall confirm an escalation process for any incident or suspicious activity.

L5.1.2 Active and passive attacks
Appropriate measures shall be in place to detect, prevent, mitigate and respond to common active and passive technical attacks. The organization shall also have agreed patching policies for digital gaming systems, whether developed and supported in house or by a third party.

L5.1.3 Network segregation
Production databases containing player or transaction data shall reside on networks separated from the servers hosting the web pages.

L5.1.4 Session identification
The user session identifier shall always be created randomly, in memory, and shall be removed after the user's session has ended.

L5.1.5 Identify points of ingress and egress
All entry and exit points to open public network systems shall be identified, monitored and controlled. The organization shall monitor all its digital gaming systems in order to prevent, detect, mitigate, and respond to cyber-attacks.

L5.1.6 Generation and storage of logs
Predefined security logs shall be generated and retained for a predefined period of time on each sensible system component in order to monitor and rectify anomalies, flaws, and alerts.

L5.1.7 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 at minimum on an annual basis.

L5.1.8 Responsible disclosure
The lottery operator shall have in place a Responsible Disclosure Policy for the disclosure of security vulnerabilities by the public to the lottery.

L5.2.2 Multiple player accounts
There shall be reasonable measures put in place to ensure each player only holds one active account.

L5.2.3 Player exclusion
There shall be an established process for excluding players in accordance with local applicable laws and/or internal procedures.

L5.2.4 Multiple payment instrument holder
There shall be an established procedure in accordance with local applicable laws, for ensuring the ownership of the payment instrument with the identity of the player so as to avoid fraud and money laundering.

L5.3.2 Game approval and modification
An approval procedure shall be defined to validate that every new game and relevant modifications on the digital gaming systems are controlled. Final game design shall be formally approved through a process involving the Security Function.

L5.3.3 Documented game procedures
Established rules shall cover design and development. In addition, game rules shall be accessible by players.

L5.3.4 Security payment methods
Objective: To protect payment methods against fraudulent uses.

L5.4.1 Data collection
Collection of sensitive data directly related to payment shall be limited to only the data strictly needed for the transaction.

L5.4.2 Payment method protection
 Adequate measures shall be in place to protect any type of payment used in the system from fraudulent use.

L5.4.3 Payment service approval
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.

L5.4.4 Transactional records related to payments
The organization shall generate all transactional records of player accounts. The data recorded shall allow the organization to trace a single financial activity of a player from another transaction.

L5.4.5 Transactional records related to payments
The organization shall generate all transactional records of player accounts. The data recorded shall allow the organization to trace a single financial activity of a player from another transaction.

L5.1.1 Layered systems architecture
The organization shall provide a layered approach to security within the digital gaming systems architecture to ensure secure storage and processing of data. Production databases containing player or transaction data shall reside on networks separated from those used by interactive services. 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.

L5.1.2 Active and passive attacks
Appropriate measures shall be in place to detect, prevent, mitigate and respond to common active and passive technical attacks. The organization shall also have agreed patching policies for digital gaming systems, whether developed and supported in house or by a third party.

L5.1.3 Network segregation
Production databases containing player or transaction data shall reside on networks separated from the servers hosting the web pages.

L5.1.4 Session identification
The user session identifier shall always be created randomly, in memory, and shall be removed after the user's session has ended.

L5.1.5 Identify points of ingress and egress
All entry and exit points to open public network systems shall be identified, monitored and controlled. The organization shall monitor all its digital gaming systems in order to prevent, detect, mitigate, and respond to cyber-attacks.

L5.1.6 Generation and storage of logs
Predefined security logs shall be generated and retained for a predefined period of time on each sensible system component in order to monitor and rectify anomalies, flaws, and alerts.

L5.1.7 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 at minimum on an annual basis.

L5.1.8 Responsible disclosure
The lottery operator shall have in place a Responsible Disclosure Policy for the disclosure of security vulnerabilities by the public to the lottery.

L5.2.1 Player account
Objective: To protect the confidentiality, integrity and availability of digital gaming systems in order to protect gaming and player data.

L5.2.2 Multiple player accounts
There shall be reasonable measures put in place to ensure each player only holds one active account.

L5.2.3 Player exclusion
There shall be an established process for excluding players in accordance with local applicable laws and/or internal procedures.

L5.2.4 Multiple payment instrument holder
There shall be an established procedure in accordance with local applicable laws, for ensuring the ownership of the payment instrument with the identity of the player so as to avoid fraud and money laundering.

L5.3.1 Documented game procedures
Established rules shall cover design and development. In addition, game rules shall be accessible by players.

L5.3.2 Game approval and modification
An approval procedure shall be defined to validate that every new game and relevant modifications on the digital gaming systems are controlled. Final game design shall be formally approved through a process involving the Security Function.

L5.3.3 Security payment methods
Objective: To protect payment methods against fraudulent uses.

L5.4.1 Data collection
Collection of sensitive data directly related to payment shall be limited to only the data strictly needed for the transaction.

L5.4.2 Payment method protection
Adequate measures shall be in place to protect any type of payment used in the system from fraudulent use.

L5.4.3 Payment service approval
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.

L5.4.4 Transactional records related to payments
The organization shall generate all transactional records of player accounts. The data recorded shall allow the organization to trace a single financial activity of a player from another transaction.

L5.4.5 Transactional records related to payments
The organization shall generate all transactional records of player accounts. The data recorded shall allow the organization to trace a single financial activity of a player from another transaction.

L5.1.1 Layered systems architecture
The organization shall provide a layered approach to security within the digital gaming systems architecture to ensure secure storage and processing of data. Production databases containing player or transaction data shall reside on networks separated from those used by interactive services. 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.

L5.1.2 Active and passive attacks
Appropriate measures shall be in place to detect, prevent, mitigate and respond to common active and passive technical attacks. The organization shall also have agreed patching policies for digital gaming systems, whether developed and supported in house or by a third party.

L5.1.3 Network segregation
Production databases containing player or transaction data shall reside on networks separated from the servers hosting the web pages.

L5.1.4 Session identification
The user session identifier shall always be created randomly, in memory, and shall be removed after the user's session has ended.

L5.1.5 Identify points of ingress and egress
All entry and exit points to open public network systems shall be identified, monitored and controlled. The organization shall monitor all its digital gaming systems in order to prevent, detect, mitigate and respond to cyber-attacks.

L5.1.6 Generation and storage of logs
Predefined security logs shall be generated and retained for a predefined period of time on each sensible system component in order to monitor and rectify anomalies, flaws, and alerts.

L5.1.7 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 at minimum on an annual basis.

L5.1.8 Responsible disclosure
The lottery operator shall have in place a Responsible Disclosure Policy for the disclosure of security vulnerabilities by the public to the lottery.

L5.2.1 Player account
Objective: To protect the confidentiality, integrity and availability of digital gaming systems in order to protect gaming and player data.

L5.2.2 Multiple player accounts
There shall be reasonable measures put in place to ensure each player only holds one active account.

L5.2.3 Player exclusion
There shall be an established process for excluding players in accordance with local applicable laws and/or internal procedures.

L5.2.4 Multiple payment instrument holder
There shall be an established procedure in accordance with local applicable laws, for ensuring the ownership of the payment instrument with the identity of the player so as to avoid fraud and money laundering.

L5.3.1 Documented game procedures
Established rules shall cover design and development. In addition, game rules shall be accessible by players.

L5.3.2 Game approval and modification
An approval procedure shall be defined to validate that every new game and relevant modifications on the digital gaming systems are controlled. Final game design shall be formally approved through a process involving the Security Function.

L5.3.3 Security payment methods
Objective: To protect payment methods against fraudulent uses.

L5.4.1 Data collection
Collection of sensitive data directly related to payment shall be limited to only the data strictly needed for the transaction.

L5.4.2 Payment method protection
Adequate measures shall be in place to protect any type of payment used in the system from fraudulent use.

L5.4.3 Payment service approval
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.

L5.4.4 Transactional records related to payments
The organization shall generate all transactional records of player accounts. The data recorded shall allow the organization to trace a single financial activity of a player from another transaction.

L5.4.5 Transactional records related to payments
The organization shall generate all transactional records of player accounts. The data recorded shall allow the organization to trace a single financial activity of a player from another transaction.

L5.5 Game design and approval
Objective: To ensure that game designs meet legal and regulatory requirements and are authorized at the appropriate level before going live.

L5.5.1 Documented game procedures
Established rules shall cover design and development. In addition, game rules shall be accessible by players.

L5.5.2 Game approval and modification
An approval procedure shall be defined to validate that every new game and relevant modifications on the digital gaming systems are controlled. Final game design shall be formally approved through a process involving the Security Function.
### L6.1 Betting framework

The framework in which the organization offers sports betting and the according rules shall be defined, maintained, and published, including but not limited to, all authorized sporting event types and betting types for each sport.

**CONSOLIDATED**

### L6.2 Events, odds and result management

**Objective:** To assure the integrity of events and their corresponding odds.

<table>
<thead>
<tr>
<th>L6.2.1</th>
<th>Events, odds and result management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedures regarding the selection of the events and for setting and updating the odds, betting margins and/or blocking events as well as for receiving the results from reliable sources shall be established. A process shall exist for validating accuracy and preventing fraudulent activities. The procedures shall be based on the respect of integrity, responsible gaming, and ensuring transparency.</td>
<td></td>
</tr>
</tbody>
</table>

**CONSOLIDATED**

| L7.1.1 | A list shall be maintained of authorized sporting event types offered for betting. |
| L7.1.2 | Maintain a list of authorized betting types for each sport offered. |
| L7.1.3 | Maintain a list of betting types per game type. Specific procedures shall be implemented in the case of nonprofessional events. |
| L7.1.4 | Maintain and make publicly available: 1) The terms of the betting offer. 2) The principles of how events are selected, how odds are set and revised based on published information and ethical rules and criteria. |

### L6.3 Monitoring for fraud and money laundering

**Objective:** To ensure actions to minimize the risk of fraud and/or money laundering.

<table>
<thead>
<tr>
<th>L6.3.1</th>
<th>Monitoring the sports betting activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedures shall be established to monitor all changes to odds and/or blocking throughout a sports event, monitoring of the market, events and customer transactions for the detection of irregularities, monitoring of winners over a certain amount of gains, and deposits over a certain size. The procedures shall also specify thresholds of payment and methods of collection. The established procedures must be in compliance with the laws of the jurisdiction within which the certifying member is domiciled.</td>
<td></td>
</tr>
</tbody>
</table>

**CONSOLIDATED**

| L7.4.1 | A procedure shall be established to monitor changes to odds and/or blocking throughout a sports event. |
| L7.4.2 | A procedure shall be established to monitor the market and detect events and/or odds irregularities. |
| L7.4.3 | 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. |
| L7.4.4 | A procedure shall be established specifying thresholds of payment and methods of collection. |
| L7.4.5 | Subject to applicable laws, a procedure shall be established to monitor winners over a certain amount of gains. |
| L7.4.6 | Establish a level above which deposits of a certain size are monitored. |

### L6.4 Sports betting

**L.6.4.1 Video Lottery Terminals (VLT)**

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

<table>
<thead>
<tr>
<th>L7.1.1</th>
<th>VLT terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLT terminals shall be maintained concerning security and prize payout percentage.</td>
<td></td>
</tr>
</tbody>
</table>

**NOT CHANGED**

| L8.1.1 | VLT terminals shall be monitored concerning security and prize payout percentage. |
| L8.1.2 | The game-rules and overall prize payout percentage shall be available to the customer. |
| L8.1.3 | Dedicated games for VLT shall be tested and a certificate to provide evidence of integrity and prize payout has to be maintained/issued. |
| L8.1.4 | There shall be documented procedures to handle dispute or protest from customer regarding a win or loss. |
| L8.1.5 | VLT system architecture The organization shall maintain a description of the overall VLT system architecture, including security measures, to ensure the integrity of the VLT game, secure storage and processing of data. |

**NEW**
5.1.1 Gaming system application security development

Objective: To ensure lottery systems are secure by design.

5.1.1.1 Application development security policies

The lottery technology supplier shall have a policy on application security across the software development lifecycle.

5.1.1.2 Static and dynamic code analysis

The lottery technology supplier shall perform static and dynamic code analysis and provide a summary of the output to the operator along with the release notes for their product for the first release and any subsequent significant release into a production environment.

5.1.1.3 Security testing

The lottery technology supplier shall perform security testing of their products and/or services, tested and configured in a way that is representative of how it will be deployed in a production environment by the operator. It shall provide a summary of the output to the operator along with the release notes for their product for the first release and any subsequent significant release into a production environment.

5.1.1.4 Secure coding practices

The lottery technology supplier shall define and require its developers to follow a set of secure coding practices and put in place measures to audit the effectiveness and compliance of those practices.

5.1.1.5 Secure coding training and awareness

The lottery technology supplier shall have a training and development program on secure coding practices for all developers that write code for gaming systems (as defined in this standard).

5.1.2 Integrity measures related to the development of gaming systems, hardware, and firmware

Objective: To ensure integrity of lottery technologies.

5.1.2.1 Release process integrity checks

The lottery technology supplier shall provide assurance over the integrity of the developed software / firmware at each stage of the development process, including any release that is not limited to, during the quality assurance process and also at the software / firmware is deployed into the production environment.

5.1.2.2 Security logging

The lottery technology supplier shall ensure adequate security logging is provided from when the developed software / firmware that can be integrated by a security team into their security toolsets to ensure the integrity of the software / firmware. The lottery technology supplier shall provide the security team with a document that details how to interpret and understand the security logging.

5.1.2.3 File integrity

The lottery technology supplier shall identity and document critical files in their product in order for the lottery operator to verify.

5.1.2.4 Hardware integrity

The lottery technology supplier shall put in place measures to allow for the identification of unauthorized attempts to alter or modify the gaming system hardware that could impact the integrity of the lottery system. In this context hardware includes any hardware, but is not limited to, video lottery terminals, lottery point of sale equipment, and random number generators. The list of any other hardware to which this control applies is to be determined through risk assessment. Hardware provisioned and hosted by the infrastructure service provider will be exempt from this control requirement.

5.1.2.5 Vulnerability and patch management

The lottery technology supplier shall ensure patches to software / firmware and any third-party code libraries used are applied in a timely manner. Whether or not patches are pushed to production gaming systems is a decision to be determined through risk management, with consideration of the lottery operator’s vulnerability and patch management policy and taking into account any commercial considerations.

5.1.2.6 Responsible disclosure

The lottery technology supplier shall have a Responsible Disclosure Policy that is available to all those who have purchased their products or services, for the disclosure of security vulnerabilities in their gaming system products.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1.3.4.4</td>
<td>Shipping security: The supplier shall ensure that ticket delivery between the supplier and the lottery is secured.</td>
</tr>
<tr>
<td>L.1.6.5</td>
<td>Parties authorized to close a game and/or destroy tickets shall be formally defined.</td>
</tr>
<tr>
<td>L.1.6.6</td>
<td>The method and control of ticket destruction shall be established.</td>
</tr>
<tr>
<td>STATUS</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NOT CHANGED</td>
<td>The control has not been changed compared to the WLA-SCS:2016</td>
</tr>
<tr>
<td>MODIFIED</td>
<td>The control has been changed compared to the WLA-SCS-2016</td>
</tr>
<tr>
<td>CONSOLIDATED</td>
<td>The control combines two or more controls from the WLA-SCS:2016. In some cases it includes also some adaptations/changes</td>
</tr>
<tr>
<td>NEW</td>
<td>The control was not present in the WLA-SCS:2016</td>
</tr>
</tbody>
</table>