World Lottery Association

WLA-SCS:2020

WLA Security Control Standard

Information and operations security and integrity requirements for lottery and sports betting operators, as well as their suppliers.

Publication: October 2020, Version 1.1
(Revised: December 10, 2020)

WORLD LOTTERY ASSOCIATION

Contents

Foreword 2

Introduction 3

1. Scope 3

2. Normative references 4

3. Terms and definitions 4

3.1 Abbreviations 4

3.2 Definitions 4

4. Overview 4

5. General security and integrity management Requirements 5

5.1 Information Security Management System (ISMS) 5

5.2 Scope of the ISMS 5

5.3 Statement of Applicability 5

Annex A (G Controls): Controls for all organizations 6

Annex B (L Controls): Controls for lottery operators 11

Annex C (S Controls): Controls for gaming system suppliers and operators 23

Annex D (M Controls): Controls for multijurisdictional games 27

Foreword

The World Lottery Association (WLA) has recognized the need for an adequate security and integrity standard for lottery and sports betting operators from its foundation and has continued to developed the work started by its predecessors.

Lottery and sports betting operators have a business need to develop environments that maintain a visible and documented security and integrity position so as to retain the confidence of players and other stakeholders alike. The WLA Security Control Standard (WLA-SCS) is designed to help lottery and sports betting operators around the world, as well as their suppliers, to achieve levels of control that are in accordance with both generally accepted information security and quality practices as well as specific industry requirements. This will support lottery and sports betting operators' increased reliance on the integrity of their operations. Certification to the WLA-SCS provides an objective measure of a lottery and sports betting operator's security control and risk management performance.

The WLA-SCS has been prepared by the WLA Security and Risk Management Committee (WLA SRMC). The WLA Security and Risk Management Committee (SRMC) consists of representatives and security specialists from lottery and sports betting operators around the world. By comparing current security and integrity practices used in the industry with those approved by lottery experts around the world, a solid security and risk management framework for lottery and sports betting operators, and their suppliers, has been established.

The WLA SRMC reviews all security control standards for use by the lottery and sports betting sector and acts as a focal point for the sector on security and risk management issues. It oversees the WLA-SCS certification process whereby compliance of WLA Members and Associate Members with the standard is verified.

All new or updated standards from the WLA SRMC must be endorsed and released by the WLA Executive Committee and approved by the delegates of the biennial General Meeting before publication.

The structure of The WLA-SCS is aligned with that of the International Standards Organization (ISO) and the WLA is committed to keeping it updated and adapted in accordance with the ISO/IEC 27001 standard.

Introduction

The WLA-SCS defines a security, integrity, and risk management standard for use by the lottery and sports betting sector and is intended to be the focal point for the sector on security and integrity issues. It describes a security management process that is aligned both with internationally recognized standards and with a common security baseline that represents good practice for lottery and sports betting operators. The standard comprises a comprehensive set of controls and requirements for lottery and sports betting operators and their suppliers.

WLA-SCS can be considered as the foundation for building trust relationships with industry stakeholders and regulators for the purpose of conducting lottery and sports betting operations or multi-jurisdictional games. It can also be of substantial assistance to top management by providing an independent review in order to foster increased confidence in the security of lottery and sports betting operations.

The latest iteration of the standard, WLA-SCS:2020, introduces a new two-level certification framework.

Compliance with the WLA-SCS Level 1 proves a basic but essential level of information security for lotteries and sports betting operators and shows their commitment to achieving WLA-SCS Level 2, the highest level of certification. WLA-SCS Level 1 certification is suitable for those WLA member organizations that wish to take a more step-by-step approach to certification.

Compliance with the WLA-SCS Level 2 allows WLA member organizations to ensure the integrity, availability, and confidentiality of services and information vital to their secure operation. Combining the assessment of controls for lottery and sports betting operators and compliance with the ISO/IEC 27001 Standard for Information Security Management Systems, WLA-SCS Level 2 represents the most complete and comprehensive certification standard for lottery and sports betting operators and their suppliers.

Adoption of the WLA-SCS is a strategic decision. The design and implementation of the organization's security and integrity management systems is influenced by their specific needs, objectives, risks and security requirements, the processes employed, and the size and structure of the organization. These factors and their supporting systems are expected to change over time and it is to be expected that a management system implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple system.

Compliance with WLA-SCS can be used by interested internal and external parties to evaluate the security and integrity of a lottery and sports betting operator's systems, as well as those of their suppliers.

In addition to ISO/IEC 27001, the WLA-SCS is aligned with ISO 9001 to allow for consistent and integrated implementation and operation with related management standards.

1. Scope

The WLA-SCS covers all types of lottery and sports betting operations, including commercial enterprises, government agencies, and non-profit organizations.

The WLA-SCS specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented security and integrity system within the context of the organization's overall risks.

The requirements set out in WLA-SCS are generic and are intended to be applicable to all organizations, regardless of type, size, and nature. Excluding any of the requirements specified in Annexes A, B, C, or D is not acceptable if an organization is to claim conformity to the WLA-SCS.

Any exclusions found to be necessary of controls in relation to Annexes A, B, C, or D need to be formally justified and evidence needs to be provided that the exclusions have been accepted by accountable persons. Where any controls are excluded, claims of conformity to WLA-SCS are not acceptable unless such exclusions do not affect the organization's ability and/or responsibility to provide security and integrity that meet the requirements as determined by a risk assessment and applicable legal or regulatory requirements. Any controls excluded from Annexes A, B, C, or D will be noted in the certification scope on the WLA-SCS certificate.

Note: If an organization already has an operational business process management system (e.g. in relation with ISO 9001 or ISO 14001), in most cases it is advisable to satisfy the requirements of the WLA-SCS within the existing management system.

Important: The WLA-SCS does not purport to include all the necessary provisions of a contract. WLA members adopting the WLA-SCS are responsible for its correct application. Compliance with any standard does not in itself confer immunity from any legal obligations.

2. Normative references

The following documents are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27001 Information Technology – Security techniques – Information Security Management Systems – Requirements.

ISO/IEC 27017 Information Technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

WLA-SCS:2020 Code of Practice – best-practices guidelines for the WLA-SCS security and integrity controls and requirements.

Guide to Certification for the WLA-SCS.

3. Terms and definitions

3.1 Abbreviations

WLA: World Lottery Association

WLA-SCS: WLA Security Control Standard

WLA SRMC: WLA Security and Risk Management Committee

3.2 Definitions

This section contains only those terms that are used in a specialized way throughout this standard. Most terms in the standard are used either according to their accepted dictionary definitions or according to commonly accepted definitions that may be found in ISO security glossaries or other well-known collections of security terms.

Assets: Information or resources to be protected by countermeasures.

Personnel: Shall be read as any employee, contractor or other third party who works for the lottery operator or lottery technology supplier and, by virtue of their role or access has the potential to impact the confidentiality, availability or integrity of the lottery.

Gaming system: Shall be read as the systems that are required to operate games, which encompasses the central gaming system and any of its peripheral components which are necessary to operate those games.

Digital gaming systems: Shall be read as all the technology that allows the offer of games via a digital sales channel.

4. Overview

The main objective of the security and integrity approach for WLA member organizations is to ensure adequate operation as well as to provide confidence.

Confidence in a lottery and sports betting operation is key to retaining players and other stakeholders. Therefore, WLA member organizations need to develop and maintain a visible and documented security and integrity environment.

The WLA SRMC has described in the WLA-SCS the requirements, control objectives and controls that are view as best practice. A lottery and sports betting organizer shall operate an information security management system that implements all requirements stated in ISO/IEC 27001, as well as the mandatory WLA-SCS requirements and controls.

The WLA-SCS incorporates baseline requirements and controls within the lottery and gaming organizer's overall security, integrity, and risk management process; avoiding overlaps with more general security frameworks. It provides lottery and gaming security and integrity professionals with a process whereby they can formally manage, update, and continuously improve their controls. Lottery and gaming organizers, therefore, need to develop and maintain a visible and documented security environment.

The WLA-SCS consists of four parts that specify the minimum controls necessary for the effective management of security and integrity in lottery and sports betting operators and suppliers to the industry.

The first part (Annex A – G Controls: Controls for all organizations) incorporates the ISO/IEC 27001 compliance within a global scope, with a further 24 basic WLA controls adjoined.

The second part (Annex B – L Controls: Controls for lottery operators) furnishes an additional 64 lottery and gaming-specific security and integrity controls representing current best practice.

The third part (Annex C – S Controls: Controls for gaming system suppliers and operators) contains 21 controls based on products and services offered by lottery and sports betting suppliers.

The fourth part (Annex D – M Controls: Controls for multi-jurisdictional games) contains 11 controls required to participate in games run by the US Multi-State Lottery Association (MUSL).

5. General security and integrity management requirements

5.1 Information Security Management System (ISMS)

Organizations certifying against WLA-SCS:2020 Level 2 shall operate an Information Security Management System (ISMS) that satisfies the requirements of ISO/IEC 27001.

5.2 Scope of the ISMS

The organization's ISMS scope shall include all lottery and gaming related activities of its operations, including all related assets and information systems. The scope may only exclude operations of the organization that are not related to the lottery and gaming activities. The excluded operations shall be fully identified and the causes for their exclusion justified in detail. General organizational functions (e.g. human resources, planning, finance …) needed to conduct lottery and sports betting operations are within the scope.

5.3 Statement of Applicability

The organization's ISMS Statement of Applicability shall explicitly include all controls in Annexes A, B, C, and D of the WLA-SCS. No control shall be excluded, although some of the controls in Annex B and C may not be applicable. Claims of non-applicability shall be justified in detail.

Excluding any of the requirements specified in this clause, as well as any control in Annexes A, B, C, and D, is not acceptable when an organization claims conformity to WLA-SCS.

Any non-applicability of controls in Annexes B and C, found to be necessary, must be formally justified and evidence shall be provided that the non-applicability has been accepted by accountable people of the organization. Where any controls are declared as non applicable, such claims are not acceptable unless the exclusions do not affect the organizations ability and/or responsibility to provide security and integrity that meets the requirements as determined by a risk assessment and applicable statutory or regulatory requirements.

Annex A (G Controls): Controls for all organizations

G.1	Organization of security	
G.1.1	**Allocation of security responsibilities**	
Objective:	To ensure that security function responsibilities are effectively implemented.	
G.1.1.1	Security forum	*Control* 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.
G.1.1.2	Security function	*Control* A security function shall exist that is 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.
G.1.1.3	Security function reporting	*Control* 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.
G.1.1.4	Security function position	*Control* It shall have the competences and be sufficiently empowered, and shall have access to all necessary resources to enable the adequate assessment, management, and reduction of risk.
G.1.1.5	Security function responsibility	*Control* The head of the security function shall be a full member of the security forum and be responsible for recommending security policies and changes.

G.2	Human resources security	
G.2.1	**Implementation of a code of conduct**	
Objective:	To ensure that a suitable code of conduct is effectively implemented.	
G.2.1.1	Code of conduct	*Control* A code of conduct shall be issued to all personnel when initially employed. All personnel shall formally acknowledge acceptance of this code.
G.2.1.2	Adherence and disciplinary action	*Control* The code of conduct shall include statements that all policies and procedures are adhered to and that infringement or other breaches of the code could lead to disciplinary action.
G.2.1.3	Conflict of interest	*Control* The code of conduct shall include statements that personnel are required to declare conflicts of interest on employment as and when they occur. Specific examples of conflict of interest shall be cited within the code.
G.2.1.4	Hospitality or gifts	*Control* The code of conduct shall address anti-graft provisions including hospitality and gifts provided by, or given to, persons or entities with which the organization transacts business.
G.2.1.5	Corporate wagering policy	*Control* There shall be an internal policy, aligned with any legislative or regulatory requirements, that addresses the right to play of personnel and those who are financially dependent on them. Where there are roles that could impact the integrity of the games without collusion they shall be prohibited from playing. Where the policy requires a prohibition of play, those roles impacted shall be explicitly defined and the prohibition shall be enforced contractually with the personnel or their employer (if not the lottery itself).
G.2.1.6	Personnel security	*Control* There shall be a policy and process for establishing trust in individuals that could impact the integrity of games through security vetting. There shall be an associated policy and process for implementing monitoring of the system activity of personnel to detect and investigate activity that might impact game integrity. These policies shall balance an individual's right to privacy with the obligation of the lottery to protect the integrity of the games.
G.2.1.7	Segregation of duties	*Control* 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.

G.2.2	Staff protection	
Objective:	To ensure that the staff are receiving an adequate level of protection.	
G.2.2.1	Policy on staff protection	*Control* 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.

G.3 Physical and environmental security

G.3.1	Secure areas	
Objective:	To ensure that access to production gaming data centers or other systems areas important for the gaming operations are adequately secured.	
G.3.1.1	Physical entry controls	*Control* 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.

G.4 Access control to gaming systems

G.4.1	User access management	
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.	
G.4.1.1	User access functions	*Control* The range of functions available to the user shall be defined in conjunction with the process owner, the IT function, and the security function.
G.4.1.2	User access logging	*Control* 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.

G.5	Information systems maintenance	
G.5.1	**Cryptographic controls**	
Objective:	To protect the confidentiality, authenticity, and integrity of cryptographic keys and important gaming, lottery, and customer related information by cryptographic means.	
G.5.1.1	Cryptographic controls for the confidentiality and integrity of data at rest on portable systems and on lottery terminals	*Control* Cryptography to protect the confidentiality of information shall be applied for sensitive information on portable computer systems (end user devices e.g. laptops, removable media e.g. USB devices, and similar) and to protect the integrity of sensitive information held at rest on lottery terminals.
G.5.1.2	Cryptographic controls for the confidentiality and integrity of data in transit over networks	*Control* 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.
G.5.1.3	Cryptographic controls for the integrity of sensitive ticket data	*Control* Cryptographic controls for integrity shall be applied for the storage of winning ticket data and validation information. This control applies to all game types.

G.5.2	**System testing**	
Objective:	To enable and conduct system testing.	
G.5.2.1	Test methodology policy and data	*Control* 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.
G.5.2.2	Gaming system security testing	*Control* Thorough testing of the gaming system security functionality shall be performed prior to production environment use and on any significant changes.

G.5.3	**Cloud security**	
Objective:	To ensure information security of lottery systems hosted in the cloud.	
G.5.3.1	Cloud security	*Control* 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.

G.6	System availability and business continuity	
G.6.1	**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.	
G.6.1.1	Availability and resilience requirements	*Control* 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.
G.6.1.2	Business Continuity	*Control* 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.

Annex B (L Controls): Controls for lottery operators

L.1	Physical instant tickets	
L.1.1	**Instant game operation**	
Objective:	To ensure that game designs and production meet legal and regulatory requirements and to ensure game integrity and prevent fraud.	
L.1.1.1	Printer/ Supplier selection	*Control* There shall be a formal approval process that involves the security function.
L.1.1.2	Integrity requirements and testing	*Control* 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 text, prize structure, protection of validation/winner files, quality controls, auditable inventory to account for the distribution, location of packs, and adequate testing of the requirements before the game is accepted.
L.1.1.3	Game data integrity	*Control* 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 / retailers.
L.1.1.4	Ticket prize confidentiality	*Control* Controls shall be in place to ensure that prior to the claiming of a prize no one in the organization has access and knowledge of which instant 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.

L.2	Lottery draws	
L.2.1	**Lottery draw management**	
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	Draw event	*Control* 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.
L.2.1.2	Draw working instructions	*Control* The organization shall publish a working instruction prior to any draw including special instructions with respect to the draw.
L.2.1.3	Draw team members	*Control* The working instruction shall include the composition of a draw team including their contact telephone numbers.
L.2.1.4	Draw team duties	*Control* The working instruction shall include the duties of the identified members of the draw team.
L.2.1.5	Reserve draw team	*Control* The working instruction shall nominate persons as reserves and detail how the reserve team are deployed.
L.2.1.6	Draw timing	*Control* The working instruction shall include the detailed timings of the draw operation from the opening of the draw location to the closing of that location.
L.2.1.7	Draw observers	*Control* The working instruction shall include details of any requirement under the lottery rules for independent observers to be present during a draw.

L.2.2	Conduct of the draw	
Objective:	To ensure that the conduct of draws is within regulatory requirements and the rules of the applicable lottery game.	
L.2.2.1	Draw procedure	*Control* 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.
L.2.2.2	Draw step-by-step guide	*Control* The draw procedure shall include a step-by-step guide of the draw process.
L.2.2.3	Draw location	*Control* The draw procedure shall include the definition of the draw location.
L.2.2.4	Draw attendance and responsibilities	*Control* The draw procedure shall include a definition of the attendance at the draw and the responsibilities and actions of all participants.
L.2.2.5	Draw supervision	*Control* The draw procedure shall define the policy regarding the attendance of an (independent) compliance officer or an auditor.
L.2.2.6	Draw operation security	*Control* The draw procedure shall include adequate security measures for the draw operation and all equipment used during the draw process.
L.2.2.7	Draw emergency	*Control* The draw procedure shall include actions in the event of an emergency occurring at any time during the course of the draw.
L.2.2.8	Draw integrity, alerting and reporting	*Control* 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.

L.2.3	**Physical drawing appliances and ball sets**	
Objective:	To ensure that physical draw appliances and ball sets meet agreed security requirements and/or regulatory specifications.	
L.2.3.1	Inspection procedure	*Control* 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.
L.2.3.2	Regular inspection and maintenance	*Control* 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.
L.2.3.3	Compatible ball sets	*Control* 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	*Control* 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	*Control* 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	*Control* 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 delay to the audio and/or video, mistakes in graphic generation or similar resulting in the public perception that there is an issue with the draw integrity.

L.2.4	Electronic lottery draws and instants	
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	*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 (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	*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	Segregation of duties	*Control* 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	
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	*Control* 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	*Control* 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 be reliant on the security of the retailer point of sale device for the integrity of lottery games.

L.4	Prize payment	
L.4.1	**Validation and payout of prizes**	
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.4.1.1	Validation process	*Control* 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 thereof.
L.4.1.2	Unique ticket reference	*Control* Each ticket for each game shall have a unique reference number.
L.4.1.3	Security of unclaimed prize data	*Control* 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, files containing information 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 or export of the data.
L.4.1.4	Prize payout procedure	*Control* 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 inquiries into the validity of claims; and a procedure with regard to late or last minute payouts.
L.4.1.5	Fraud detection	*Control* There shall be adequate audit records kept and reviewed as part of the prize payout procedure to identify unusual patterns of late payouts and any claims made by retailers or personnel that might require investigation.

L.5	Digital sales channels and interactive services	
L.5.1	**Digital gaming systems**	
Objective:	To protect the confidentiality, integrity and availability of digital gaming systems in order to protect gaming and player data.	
L.5.1.1	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.5.1.2	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 also have agreed patching policies for digital gaming systems, whether developed and supported in house or by a third party.
L.5.1.3	Network segregation	*Control* Production databases containing player or transaction data shall reside on networks separated from the servers hosting the web pages.
L.5.1.4	Session information	*Control* The user session identifier shall always be created randomly, in memory, and shall be removed after the user's session has ended.
L.5.1.5	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.5.1.6	Generation and storage of logs	*Control* 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.
L.5.1.7	Security testing	*Control* 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.
L.5.1.8	Responsible disclosure	*Control* The lottery operator shall have in place a Responsible Disclosure Policy for the disclosure of security vulnerabilities by the public to the lottery.

L.5.2	Player account	
Objective:	To protect the player and to manage the risk of fraud and money laundering.	
L.5.2.1	Player account	*Control* 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.
L.5.2.2	Multiple player accounts	*Control* There shall be reasonable measures put in place to ensure each player only holds one active account.
L.5.2.3	Player exclusion	*Control* There shall be an established process for excluding players in accordance with local applicable laws and/or internal procedures.
L.5.2.4	Multiple payment instrument holder	*Control* There shall be an established procedure, in accordance with local applicable laws, for assuring the ownership of the payment instrument with the identity of the player so as to avoid fraud and money laundering.

L.5.3	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.	
L.5.3.1	Documented game procedures	*Control* Established rules shall cover design and development. In addition, game rules shall be accessible by players.
L.5.3.2	Game approval and modification	*Control* An approval procedure shall be defined to validate that every new game and relevant modifications on the digital gaming systems are controlled. Final game design shall be formally approved through a process involving the Security Function.

L.5.4	Securing payment methods	
Objective:	To protect payments methods against fraudulent uses.	
L.5.4.1	Data collection	*Control* Collection of sensitive data directly related to payment shall be limited to only the data strictly needed for the transaction.
L.5.4.2	Payment method protection	*Control* Adequate measures shall be taken in order to protect any type of payment used in the system from fraudulent use.
L.5.4.3	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.5.4.4	Transactional records related to payments	*Control* 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.

L.6	Sports betting	
L.6.1	**Selecting the offer**	
Objective:	To ensure the integrity of a betting offer.	
L.6.1.1	Betting framework	*Control* 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.

L.6.2	**Events, odds and result management**	
Objective:	To assure the integrity of events and their corresponding odds.	
L.6.2.1	Events, odds and result management	*Control* 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.
L.6.2.2	Live betting	*Control* There shall be documented procedures to assure and monitor the integrity of the live bet offering, the results handling and customer protection. Indicative areas for consideration in the procedure for results handling shall include, but not be limited to, time delays, sources of results, and reversal of results. The procedures shall also account for courtsiding prevention mechanisms including but not limited to a delay in live pictures.
L.6.2.3	Safeguarding payout levels	*Control* The organization shall establish a set of measures to ensure authorized payout levels are not exceeded.

L.6.3	**Monitoring for fraud and money laundering**	
Objective:	To ensure actions to minimize the risk of fraud and/or money laundering.	
L.6.3.1	Monitoring the sports betting activities	*Control* 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.

L.7	Interactive Video Lottery Terminals	
L.7.1	**Video Lottery Terminals (VLT)**	
Objective:	To ensure secure operation of all VLT terminals no matter which system design or operating models.	
L.7.1.1	VLT terminals	*Control* VLT terminals shall be monitored concerning security and prize payout percentage.
L.7.1.2	VLT games	*Control* The game-rules and overall prize-payout percentage shall be available to the customer.
L.7.1.3	VLT game certificate	*Control* Dedicated games for VLT shall be tested and a certificate to provide evidence of integrity and prize-payout has to be maintained/issued.
L.7.1.4	VLT incidents	*Control* There shall be documented procedures to handle dispute or protest from customer regarding a win or loss.
L.7.1.5	VLT system architecture	*Control* 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.

Annex C (S Controls): Controls for gaming system suppliers and operators

The S controls apply to gaming systems (as defined in this standard) and shall be in the certification scope of whichever organization develops the gaming system and/or manages the gaming system – whether that be a technology supplier or the operator's own in-house developers.

S.1	**Lottery systems security assurance**	
S.1.1	**Gaming system application security development**	
Objective:	To ensure lottery systems are secure by design.	
S.1.1.1	Application development security policy	*Control* The lottery technology supplier shall have a policy on application security across the software development lifecycle.
S.1.1.2	Static and dynamic code analysis	*Control* 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.
S.1.1.3	Security testing	*Control* The lottery technology supplier shall perform security testing of their products and/or services, hosted 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.
S.1.1.4	Secure coding practices	*Control* 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.
S.1.1.5	Secure coding training and awareness	*Control* The lottery technology supplier shall have a training and awareness program on secure coding practices for all developers that write code for gaming systems (as defined in this standard).

S.1.2	**Integrity measures related to the development of gaming system hardware, software, and firmware**	
Objective:	To ensure integrity of lottery technologies.	
S.1.2.1	Release process integrity checks	*Control* The lottery technology supplier shall provide assurance over the integrity of their developed software / firmware at each stage of the development process, including as a minimum but not limited to, during the quality assurance process and also as the software / firmware is deployed into the production environment.
S.1.2.2	Security logging	*Control* The lottery technology supplier shall ensure adequate security logging is provided from their developed software / firmware that can be integrated by a security team into their security toolsets to ensure the integrity of the lottery software/ firmware. The lottery technology supplier shall provide the security team with a document that details how to interpret and understand the security logging.
S.1.2.3	File integrity	*Control* The lottery technology supplier shall identify and document critical files in their product in order for the lottery operator to verify the integrity of the production environment.
S.1.2.4	Hardware integrity	*Control* The lottery technology supplier shall put in place measures to allow for the identification of unauthorized attempts to add or modify the gaming system hardware that could impact the integrity of the lottery system. In this context hardware includes as a minimum, but is not limited to, video lottery terminals, lottery point of sale equipment, and random number generators. The exact list of hardware to which this control applies is to be determined through risk assessment. Hardware provisioned and hosted by an Infrastructure as a Service provider will be exempt from this control requirement.
S.1.2.5	Vulnerability and patch management	*Control* The lottery technology supplier shall ensure there is a process through which updates to software / firmware and any third-party code libraries used can be applied in a timely manner. Whether or not patches are pushed to production gaming systems is a decision to be determined via risk assessment, with consideration of the lottery operator's vulnerability and patch management policy and taking into account any commercial considerations.
S.1.2.6	Responsible disclosure	*Control* 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.

S.1.3	**Integrity measures related to printing of physical instant tickets**
Objective:	To ensure the integrity of physical instant tickets.

S.1.3.1	Physical instant game requirements	
Objective:	To align lottery requirements to supplier specification.	
S.1.3.1.1	Instant game requirements	*Control* The supplier shall formally validate requirements with the lottery and translate those requirements into specifications; any change in the specifications shall follow both supplier's and lottery's change management process.

S.1.3.2	Creating and validating the data	
Objective:	To ensure that instant game programming matches requirements and is kept secured.	
S.1.3.2.1	Instant game data generation	*Control* The randomization process used for the generation of instant game data is subject to the application of WLA-SCS L.2.4 electronic lottery draws and instants controls and the requirements agreed between the operator and supplier.
S.1.3.2.2	Game data validation	*Control* The supplier shall ensure that an independent team validates logical game data against lottery requirements. Reports with results shall be made available to the lottery.
S.1.3.2.3	Data confidentiality	*Control* The supplier shall ensure that access to validation data is restricted at all times, even after instant game delivery, in conformity with the principle of least privilege.

S.1.3.3	Printing	
Objective:	To ensure integrity features in the printing process.	
S.1.3.3.1	Validation before printing	*Control* The supplier shall formally validate the final visuals and texts with the lottery before printing tickets.
S.1.3.3.2	Integrity checks	*Control* The supplier shall perform integrity audits on tickets on a regular basis.

S.1.3.4	Finishing	
Objective:	To ensure conformity with prize structure and to guarantee ticket integrity during shipment.	
S.1.3.4.1	Unique ticket reference number	*Control* Provisions shall be made for each ticket delivered to have a unique reference number.
S.1.3.4.2	Prize structure conformity	*Control* The supplier shall provide evidence that in each printing lot they have supplied the correct number of tickets in accordance with the required prize structure.
S.1.3.4.3	Scrapped tickets	*Control* There shall be a documented procedure to ensure that undelivered printed tickets are securely destroyed.
S.1.3.4.4	Shipping security	*Control* The supplier shall ensure that ticket delivery between the supplier and the lottery is secured.

Annex D (M Controls): Controls for multijurisdictional games

M.1	Requirements to participate in games run by the Multi-State Lottery Association (MUSL)	
M.1.1	**Security, integrity and availability of transactions**	
Objective:	To ensure that transactions are properly recorded and secured.	
M.1.1.1	Claim Validations	*Control* To meet the requirement of the controls listed in section L.4.1 of this document, an organization shall additionally comply with the MUSL Minimum Game Security Standards.
M.1.1.2	Redundancy of transaction data	*Control* Records of sold transaction data on the computer gaming system shall exist in no fewer than two distinct datacenter locations and shall be sufficiently separated so as not to be subject to the same disaster event.
M.1.1.3	Acknowledgement of transaction	*Control* Each location shall receive and acknowledge transaction board data prior to a ticket being allowed to print.
M.1.1.4	Backup of play data	*Control* Play data must be backed up daily and stored offline and offsite.
M.1.1.5	Integrity of transactions before and after a draw	*Control* A MUSL-approved cryptographic hash function shall be applied to the entire set of transactions stored via the internal control system (ICS) pre-draw for each draw to create a message digest of hash. The same cryptographic hash function shall be re-applied to the entire set of transactions after the creation of a winner by tier report immediately following a drawing.

M.1.2	Security of retailer point of sale device	
Objective:	To ensure the security of retailer point of sale devices that are not dedicated lottery terminals.	
M.1.2.1	Retailer point of sale device	*Control* Where a retailer point of sale device is used instead of a dedicated lottery terminal, the retailer point of sale device must meet NASPL requirements.
M.1.2.2	Lottery terminals not intended to produce live tickets	*Control* Terminals not intended to produce live tickets, and that are accessible to computer gaming system or internal control system operators, shall be modified in such a manner as to make it clear that any ticket created by such terminals is not valid. Neither site operations nor IT personnel shall be able to circumvent modifications.

M.1.3	Quick picks	
Objective:	To ensure that quick picks are selected randomly.	
M.1.3.1	Randomness of quick picks	*Control* Software used to generate random numbers for quick picks shall comply with WLA-SCS control L.2.4.3 “Electronic draw randomness and integrity verification”.

M.1.4	Separation between ICS and CGS	
Objective:	To ensure segregation between the Computer Gaming System (CGS) and the Internal Control System (ICS).	
M.1.4.1	Separation between the computer gaming system and the internal control system	*Control* With regard to WLA-SCS control L.2.2.8 “Independent Control System”, if the computer gaming system is run by a third-party vendor, the ICS must be operated by a separate organization. In any case, responsibility for these systems must be highly separated, and no one individual can have access or partial access to both the ICS and CGS systems.

M.1.5	Draw process	
Objective:	To ensure continuity and integrity between the processing of winning numbers and the processing of sales transactions.	
M.1.5.1	Usage of same personnel and internal control system.	*Control* The lottery or its authorized designee shall process winning numbers using the same personnel and the same ICS systems used for processing sales transactions.

M.1.6	Intrusion detection system	
Objective:	To manage the risk of cyberattack to the ICS and CGS.	
M.1.6.1	Intrusion detection system on ICS and CGS networks	*Control* Intrusion detection and reporting or an intrusion prevention system shall be in place on both the ICS and CGS networks and actively configured to notify local administrators.