World Lottery Association

WLA Security Control Standard

Information and operations security and integrity requirements for lottery and gaming organizations

WLA-SCS:2016

Edition November 2016 (rev)

World Lottery Association

WLA Security Control Standard

Information and operations security and integrity requirements for lottery and gaming organizations

WLA-SCS:2016

Corrigenda of types and corrections in L.2.4.3, L.8.1 and L.8.1.3.

Contents

List of Tables

Foreword

The World Lottery Association (WLA) has recognized the need for an adequate security and integrity standard for lottery and gaming organizers from its foundation and has developed further the work started by its predecessors.

Lottery and gaming organizers 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 gaming organizers around the world 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 a lottery and gaming organizer's increased reliance on the integrity of their lottery operations. Certification to the WLA-SCS provides an objective measure of a lottery and gaming organizer'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 SRMC includes representatives and security specialists from lottery and gaming organizers from 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 gaming organizers has been established.

The WLA SRMC reviews all security control standards for use by the lottery and gaming sector, acts as a focal point for the sector on security issues and oversees the certification process whereby lottery and gaming organizers' compliance with the WLA-SCS is verified.

All new or updated standards from the WLA SRMC have to be endorsed and released by the WLA Executive Committee and approved by the General Meeting before publication as a WLA standard.

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

0 Introduction

0.1 General

This standard defines a security, integrity and risk management standard for use by the lottery and gaming sector and is intended to be the focal point for the sector on security and integrity issues. It is intended to assist lottery and gaming organizers around the world towards attaining a level of control in line with generally accepted practices and makes possible an increased reliance on the integrity of lottery operations.

This standard describes a security management process that is aligned both with internationally recognized standards and with a common security baseline for specific aspects relating to lottery and gaming organizers which represent good practice. It comprises a comprehensive set of requirements, controls and standards for lottery and gaming organizers, including conformity with all the requirements stated in ISO/IEC 27001 Standard for Information Security Management Systems.

It can also be considered as the foundation for building trust relationships with other lottery and gaming organizers, stakeholders and regulators for the purpose of conducting lottery and gaming operations or multi-jurisdictional games and can be of substantial assistance to management by providing an independent review to build increased confidence in the security of a lottery. Compliance with the WLA-SCS allows a lottery and gaming organizer to ensure the integrity, availability, and confidentiality of services and information vital to their secure operation.

The adoption of the WLA-SCS is a strategic decision for a lottery and gaming organizer. 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 gaming organizer's systems.

0.2 Compatibility With Other Management Systems

The WLA-SCS is aligned with ISO/IEC 27001 and ISO 9001 to allow for consistent and integrated implementation and operation with related management standards. As a result, a single, suitably designed management system can satisfy the requirements of all these ISO and WLA standards.

1 Scope of the Standard

1.1 General

The WLA-SCS covers all types of lottery and gaming organizations 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. It specifies the requirements for the implementation of security and integrity controls applicable to the needs of individual organizations, so that the security and integrity management systems can be designed to ensure the selection of adequate and proportionate security and integrity controls that protect assets and give confidence to interested parties.

1.2 Application

The requirements set out in WLA-SCS are generic and are intended to be applicable to all lottery and gaming organizations, regardless of type, size and nature.

In any case, excluding any of the requirements specified in Clauses 5, 6 and 7 and controls in Annexes A and B is not acceptable when an organization claims conformity to the WLA-SCS.

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. Lottery and gaming organizers adopting 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, in whole or in part, are normatively referenced in this document and are indispensable for its application: ISO/IEC 27001 Information Technology – Security techniques – Information Security Management Systems – Requirements.

3 Terms and Definitions

3.1 Common Abbreviations

The following abbreviations are common to more than one part of this standard:

WLA: World Lottery Association

WLA-SCS: WLA Security Control Standard

WLA SRMC: Security and Risk Management Committee of the World Lottery Association

3.2 Definitions

This section contains only those terms that are used in a specialized way throughout this standard. The majority of 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.

WLA (World Lottery Association): A member-based global trade organization made up of lottery and gaming organizers from over 80 countries in five continents. The WLA is committed to sharing knowledge and experience amongst its members and to improving their business in the interest of stakeholders as determined by the authorities in their respective jurisdictions.

WLA SRMC (Security and Risk Management Committee): A committee of security professionals from lottery and gaming organizations of six different continents, whose members are duly appointed by the WLA Executive Committee. The WLA SRMC accredits auditors, after checking requirement fulfilment, to perform WLA-SCS conformance audits, and advises the WLA and its Members on security and risk management issues.

4 Overview

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

Confidence in a lottery operation is key to retaining players and other stakeholders. Lottery and gaming organizers, therefore, 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 seen as best practice. A lottery and gaming organizer shall operate an information security management system that implements all requirements stated in ISO/IEC 27001, as well as the mandatory 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, besides requirements stated in Clause 5, includes two annexes that specify the minimum controls necessary for the effective management of security and integrity in a lottery and gaming organization.

Annex A – General Security and Integrity Control Objectives and Controls, includes general information security and integrity controls, that enhance and refine ISO/IEC 27001, with a further 23 controls. Those are the so called "G" (from general) controls.

Annex B – Lottery and Gaming Specific Security and Integrity Control Objectives and Controls, furnishes an additional 114 lottery and gaming-specific security and integrity controls representing current best practice. Those are the so called "L" (from Lottery) controls.

5 General Security and Integrity Management Requirements

5.1 Information Security Management System

The organization 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. These operations excluded shall be fully identified and the causes for exclusion justified in detail. General organizational functions (e.g. human resources, planning, finance...) needed to produce the lottery and gaming 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 and B of the WLA-SCS. No control shall be excluded, but some of the controls in Annex B may be non-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 and B, is not acceptable when an organization claims conformity to WLA-SCS.

Any non-applicability of controls of Annex B found to be necessary needs to be formally justified and evidence needs to be provided that the non-applicability has been accepted by accountable people of the organization. Where any controls are non-applicable, claims are conformity are not acceptable unless such 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.

6 General Security and Integrity Control Objectives and Controls

The organization shall implement the 23 general controls described in clauses G.1 to G.6 in Annex A.

7 Lottery and Gaming Specific Security and Integrity Control Objectives and Controls

The organization shall implement the 114 lottery specific controls, Clauses L.1 to L.8 in Annex B, if applicable.

Annex A
("G" Controls)
(normative)

General Security and Integrity Control Objectives and Controls

The control objectives and controls listed in *Table A,* Clauses G.1 to G.6, are mandatory controls under the WLA-SCS. They have been derived from control objectives and controls listed in ISO/IEC 27001 to extend the WLA-SCS beyond the ISO standard. The elements in *Table A* are not exhaustive and a lottery and gaming organization may consider that additional control objectives and controls are necessary.

Table A – Control Objectives and Controls

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 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 infra-structure, and game processes.
G.1.1.3	Security function reporting	*Control* The security function shall report to no lower than executive level management and not reside within or report to the IT function.
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 employees 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	Policy on hospitality or gifts	*Control* The code of conduct shall include an anti-graft policy also including hospitality and gifts provided by or given to persons or entities with which the organization transacts business.

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 have a two-factor authentication process. Single-factor electronic access control methods are acceptable if the area is staffed at all times.

G.4	Access control to gaming systems	
G.4.1	**Remote user access management**	
Objective:	To ensure authorized remote user access and to prevent unauthorized access to gaming systems.	
G.4.1.1	Remote user access to gaming systems	*Control* A procedure for strictly controlled remote access shall be established.
G.4.1.2	Remote 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.4.1.3	Remote user access logging	*Control* All actions performed through remote user access shall be logged and these logs shall be regularly reviewed.

G.5	Information systems maintenance	
G.5.1	**Cryptographic controls**	
Objective:	To protect the confidentiality, authenticity, and integrity of important gaming, lottery, and customer related information by cryptographic means.	
G.5.1.1	Cryptographic controls for data on portable systems	*Control* Encryption shall be applied for non-public organization data on portable computer systems (laptops, USB devices, etc.).
G.5.1.2	Cryptographic controls for networks	*Control* 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.
G.5.1.3	Cryptographic controls for storage	*Control* Integrity measures shall be applied for the storage of winning information ticket data and validation information.
G.5.1.4	Cryptographic controls for validation numbers	*Control* Encryption shall be applied for instant ticket validation numbers.
G.5.1.5	Cryptographic controls for payment orders	*Control* Encryption shall be applied for financial transactions between the organization and a banking institution.

G.5.2	System testing	
Objective:	To maintain the security, confidentiality, and integrity of test data.	
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 personal information.

G.6 Business continuity management

G.6.1	Press media handling and availability	
Objective:	To ensure the protection of the organization's image and reputation and to counteract interruptions to business activities.	
G.6.1.1	Press media and personnel handling	*Control* The business continuity plan shall include plans to handle the media and personnel during crisis situations.
G.6.1.2	Shareholder or board approval	*Control* The organization shall ensure that the board or shareholders of the organization agree to the decided availability requirements.

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

Annex B
("L" Controls)
(normative)

Lottery and Gaming Specific Security and Integrity Control Objectives and Controls

The control objectives and controls listed in *Table B,* Clauses L.1 to L.8, are mandatory unless not applicable to a lottery and gaming organization's operations. The elements in *Table B* are not exhaustive and a lottery and gaming organization may consider that additional control objectives and controls are necessary.

Table B – Lottery and Gaming Specific Security and Integrity Control Objectives and Controls

L.1	**Instant tickets**	
L.1.1	**Instant game design**	
Objective:	To ensure that game designs meet legal and regulatory requirements and are authorized at the appropriate level before going into production.	
L.1.1.1	Documented instant ticket procedures	*Control* Formal procedures shall be established covering the design, development, production, and release of instant games.
L.1.1.2	Game design approval	*Control* Final game design shall be formally approved through a process involving the security function.
L.1.1.3	Supplier selection	*Control* Printers/suppliers of instant tickets shall be subject to a selection and approval process. The approval process shall involve the security function.
L.1.1.4	Security requirements	*Control* 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.
L.1.1.5	Quality control	*Control* Quality control requirements for printing instant tickets shall be documented and form part of the contract with the supplier/printer.
L.1.1.6	Policy on audits and laboratory testing	*Control* A policy shall be established describing the required audits and laboratory testing of game design and ticket printing.

L.1.2	**Instant ticket printing**	
Objective:	To ensure that instant tickets comply with the organization's security standards for production and printing.	
L.1.2.1	Instant ticket printing requirements	*Control* The organization shall provide the printer/supplier with a detailed game specification and detailed security requirements.
L.1.2.2	Printing quality assurance	*Control* Security requirements shall include a requirement for the supplier/printer's internal quality assurance function.
L.1.2.3	Encrypted validation numbers	*Control* Security requirements shall include validation numbers that employ encryption techniques.
L.1.2.4	Encrypted validation and winner files	*Control* Security requirements shall include validation files and winner information to be stored using encryption techniques.
L.1.2.5	Ticket verification	*Control* Checks of random samples of ticket packs for each game shall be carried out to ensure that games conform to the tolerances set out in the organization's specification.
L.1.2.6	Acceptance testing of data	*Control* Security requirements shall include that after the first print run and before launch, inventory and validation data is provided to the appointed organization's security or quality assurance function for acceptance testing.

L.1.3	**Shipment of instant tickets**	
Objective:	To ensure the secure transportation of instant tickets from the printer/supplier to the organization.	
L.1.3.1	Shipping manifest	*Control* Shipping requirements shall specify that a complete shipping manifest shall be sent to the organization before a consignment is dispatched.
L.1.3.2	Transportation method	*Control* The organization shall ensure that the shipment process in accordance with an agreed (either through a direct agreement or through an agreement with the supplier) method of transportation that is not to be varied without the authority of the organization.
L.1.3.3	Sealed transport containers	*Control* Shipping containers shall be sealed and seal numbers recorded on manifests.

L.1.4	Storage and distribution of instant tickets	
Objective:	To ensure that instant tickets are stored and distributed in a secure manner.	
L.1.4.1	Storage facility audits	*Control* A procedure shall be established to provide for authorized personnel to inspect instant ticket storage facilities at least annually.
L.1.4.2	Ticket transport verification	*Control* Each consignment of instant tickets shall be formally verified on arrival.
L.1.4.3	Ticket verification procedure	*Control* An arrival verification procedure shall ensure that seal numbers are correct and that the security of the container has been maintained.
L.1.4.4	Ticket verification outcome	*Control* The verification outcome shall be documented and in case of non-conformities and/or irregularities action shall be taken to determine whether the security of a consignment has been compromised.
L.1.4.5	Instant ticket control system	*Control* A control system shall be in place to account for packs of instant tickets from the time they arrive at the organization's storage facilities to the time they arrive at the retailer.

L.1.5	Retailer security – instant tickets	
Objective:	To ensure that retailers conform to the security requirements applicable to the receipt, storage and sale of instant tickets.	
L.1.5.1	Instant ticket receipt by retailers	*Control* The organization shall require retailers, either via contract or other means, to validate the integrity of packages of instant tickets on receipt and to confirm that they have received a particular consignment of tickets.
L.1.5.2	Receipt confirmation	*Control* Upon receipt confirmation, the tickets shall be formally recorded as having been issued to that retailer.
L.1.5.3	Retailer instructions	*Control* The organization shall provide retailers with instructions regarding prize claim payout, ticket validation, instant ticket handling and storage, reporting of security issues, and the handling of lost and stolen tickets.
L.1.5.4	Retailer security training	*Control* The organization shall provide and document training for retailers to enable them to meet the security requirements for handling instant tickets.

L.1.6	**Instant game closures**	
Objective:	To ensure that security control and audit requirements are maintained when an instant game is closed.	
L.1.6.1	Game closure procedure	*Control* The organization shall establish a game closure procedure to be used in the closing of an instant game.
L.1.6.2	Retailer information	*Control* The method and timing of informing retailers of a game closure and the collection of unused tickets shall be established and documented.
L.1.6.3	Balance of ticket stock	*Control* A procedure to be used to balance game tickets held in storage and by retailers shall be established.
L.1.6.4	Stock audit check	*Control* Requirements for audit checks of instant ticket stock shall be established and documented.
L.1.6.5	Authorized parties	*Control* Parties authorized to close a game and/or destroy tickets shall be formally defined.
L.1.6.6	Ticket destruction	*Control* The method and control of ticket destruction shall be established.

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.2.3	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.2.4	Electronic Lottery Draws	
Objective:	To ensure electronic drawing system integrity by physical and logical protection.	
L.2.4.1	Physical and logical protection of the technical system	*Control* Measures shall be taken in order to ensure only those authorized have physical access to, and logical protection of, both the Random Number Generator (entropy source) and the drawing algorithm in order to prevent any modification of the algorithm and the entropy source settings. The physical system(s) 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	Separation of duties	*Control* A specific procedure shall be implemented concerning separation of duties involved in an electronic draw in order to prevent any internal fraud. Notably no one person should be allowed to perform more than one of the following types of duties: maintaining, monitoring or performing draws on electronic gaming equipment.

L.3 Retailer security

L.3.1	Recruitment and set-up	
Objective:	To ensure that only approved people, operating in approved locations, are accepted as retailers to sell the organization's products on and off-line.	
L.3.1.1	Retailer contract	*Control* Retailers shall be engaged under the terms of an agreed contract.

L.3.2	Retailer operations	
Objective:	To ensure that retailer operations, whether on or off-line, conform to the organization's security requirements.	
L.3.2.1	Retailer security	*Control* To enable retailers to conform to organizational security requirements, the organization shall specify a security environment the retailer is required to operate.

L.3.3	**Gaming terminal security**	
Objective:	To ensure the adequacy of gaming terminal security.	
L.3.3.1	Transaction security	*Control* The data traffic between the gaming terminals and the central computer gaming system shall be protected.
L.3.3.2	Terminal security testing	*Control* Thorough testing of terminal security functionality shall be performed prior to production environment use. This testing shall include provisions that the correct version of software is in place.
L.3.3.3	Self-service terminal security	*Control* Self-service terminals shall have security mechanisms in place to protect game integrity.

L.4	**Prize money protection**	
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.	
L.4.1.1	Validity of winning information	*Control* The organization shall implement procedures to ensure the validity of winning transactions, claims and/or tickets.
L.4.1.2	Validation processes	*Control* The organization shall define and document validation processes for different prize levels and types of game.
L.4.1.3	Prize payout	*Control* The organization shall establish a process for payment or transfer of prizes.

L.4.2	**Unclaimed prize money**	
Objective:	To secure unclaimed prize money before and after the end of the prize claim period.	
L.4.2.1	Unique ticket reference number	*Control* Provisions shall be made in the on-line production system for each ticket issued to have a unique reference number.
L.4.2.2	Procedure for the protection of unclaimed prize money	*Control* The organization shall establish a procedure specifically related to the protection of unclaimed prize money and data files containing information relating to the payout status of each game, the specific transactions yet to be claimed and the validation files.
L.4.2.3	Prize payout period and auditing	*Control* The procedure shall cover the entire prize payout period as well as the auditing of the final transfers upon game settlement.
L.4.2.4	Payout rules and inquiries	*Control* The procedure shall confirm the rules covering ticket validity time, payout on lost and defaced tickets, inquiries into the validity of claims and late or last minute payouts.
L.4.2.5	Unclaimed prize information access control	*Control* The procedure shall confirm that access control be strict and limited to that required in respect of records of unclaimed prizes.
L.4.2.6	Access reporting	*Control* The procedure shall confirm a reporting process in case of unauthorized access attempts.
L.4.2.7	Escalation process	*Control* The procedure shall confirm an escalation process for any incident or suspicious activity.
L.4.2.8	Audits of access log information	*Control* The procedure shall confirm that unclaimed prize money is secured.
L.4.2.9	Audit trails	*Control* The procedure shall confirm audit trails are able to identify unusual patterns of late payouts.

L.5	Sales staff and customer services	
L.5.1	**Staff working outside organization premises**	
Objective:	To ensure that sales representatives and technicians working outside of lottery premises are receiving an adequate level of protection.	
L.5.1.1	Staff working outside of organization premises	*Control* A policy shall be established to ensure that staff working outside lottery premises are receiving and implementing an adequate level of protection.

L.5.2	**Customer service areas**	
Objective:	To ensure that the customer service and prize claim areas are receiving an adequate level of protection.	
L.5.2.1	Staff working in sensitive areas with public access	*Control* A policy shall be established to ensure that staff working in sensitive areas with public access are receiving an adequate level of protection.

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

L.6.2	**Player account**	
Objective:	To protect the player and to fight fraud and money laundering.	
L.6.2.1	Player identification and data protection	*Control* There shall be a formal process for identification of player. Both player data and the wallet shall be considered as critical assets for the purposes of risk assessment.
L.6.2.2	Multiple player accounts	*Control* There shall be an established procedure for the use of multiple player accounts whenever this does not exist only one account per player shall be allowed.
L.6.2.3	Players exclusion	*Control* There shall be an established process for excluding players in accordance with local applicable laws and/or internal procedures.
L.6.2.4	Multiple payment instrument holder	*Control* There shall be an established procedure for assuring the match of ownership between the payment type holder and the player account holder.

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

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

L.7	**Sports betting**	
L.7.1	**Selecting the offer**	
Objective:	To ensure integrity of the betting offer.	
L.7.1.1	Authorized events list	*Control* A list shall be maintained of authorized sporting event types offered for betting.
L.7.1.2	Authorized betting types list	*Control* Maintain a list of authorized betting types for each sport offered.
L.7.1.3	Authorized betting options list	*Control* Maintain a list of betting types per game type. Specific procedures shall be implemented in the case of nonprofessional events.
L.7.1.4	Betting offering information	*Control* 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.

L.7.2	**Events and Odds management**	
Objective:	To assure the integrity of events and their corresponding odds.	
L.7.2.1	Selection of events	*Control* A procedure to select events based on the authorized events list shall be established to assure the integrity of the offering.
L.7.2.2	Setting and updating the odds	*Control* There shall be established procedures for setting and updating the odds and/or blocking events, taking into account market forces. A process shall exist for validating accuracy and preventing fraudulent activities. The procedures shall be based on respect of integrity, responsible gaming, and ensuring transparency.
L.7.2.3	Setting of the betting margin	*Control* Authorized levels for the margin of each bet type shall be documented and approved.
L.7.2.4	Safeguarding payout levels	*Control* The organization shall establish a set of measures to ensure authorized payout levels are not exceeded.

L.7.3	**Results handling**	
Objective:	To ensure reliance on reliable results.	
L.7.3.1	Results for completed events	*Control* There shall be a policy for the confirmation of results based on qualified and approved sources, before publicly announcing results and declaring winners.
L.7.3.2	Results records	*Control* A backup record of all results shall be kept and identified as a critical asset.

L.7.4	**Monitoring for fraud and money laundering**	
Objective:	To ensure actions to minimize the risk of fraud and/or money laundering.	
L.7.4.1	Odds monitoring	*Control* A procedure shall be established to monitor all changes to odds and/or blocking throughout a sports event.
L.7.4.2	Market monitoring	*Control* A procedure shall be established to monitor the market and detect events and/or odds irregularities.
L.7.4.3	Customer transaction monitoring	*Control* There shall be procedures in place to detect betting irregularities, including regional patterns. In case of detection a process shall be in place to notify the regulatory authority and if necessary the relevant sport governing body.
L.7.4.4	Cash payment of winnings	*Control* A procedure shall be established specifying thresholds of payment and methods of collection.
L.7.4.5	Winners monitoring	*Control* Subject to applicable laws, a procedure shall be established to monitor winners over a certain amount of gains.
L.7.4.6	Deposit monitoring	*Control* Establish a level above which deposits of a certain size are monitored.

L.7.5	**Live betting**	
Objective:	To ensure the propriety of the offering of bets during game time.	
L.7.5.1	Event integrity monitoring	*Control* There shall be established procedures to assure and document the integrity of the live bet offering.
L.7.5.2	Results handling in live offerings	*Control* There shall be established procedures to assure and document the integrity of results during the live bet offering. Indicative areas for consideration are time delay, sources for results, reversal of results, etc.
L.7.5.3	Courtsiding prevention mechanisms	*Control* Ensure customer protection and fraud/integrity protection through the provision of a safety mechanism to account for delay in live pictures.

L.7.6	**Duties separation and internal control**	
Objective:	To avoid internal collusions.	
L.7.6.1	Duties separation	*Control* There shall be a separation of duties to ensure that no group has overall control without oversight.
L.7.6.2	Corporate betting policy	*Control* There shall be an internal policy addressing employees' rights to play.

L.8	**Interactive Video Lottery Terminals (VLT)**	
L.8.1	**Video Lottery Terminals (VLT)**	
Objective:	To ensure secure operation of VLT terminals no matter which system design or operating models.	
L.8.1.1	VLT terminals	*Control* VLT terminals shall be monitored concerning security and prize payout percentage.
L. 8.1.2	VLT games	*Control* The game-rules and overall prize-payout percentage shall be available for the customer.
L.8.1.3	VLT game certificate	*Control* Dedicated games for VLT shall be tested and a certificate to provide evidence of integrity has to be maintained/issued.
L.8.1.4	VLT incidents	*Control* There shall be documented procedures to handle dispute or protest from customer regarding a win or loss.

World Lottery Association

WLA Security Control Standard

Information and operations security and integrity requirements for lottery and gaming organizations

WLA-SCS:2016