WORLD LOTTERY ASSOCIATION

Code of Practice for the WLA-SCS:2024 CoP:2024

Foreword

Introduction

Scope

Normative references

Terms and definitions

Annex A (G Controls) Organizational Controls

- G.1 Organization of security
- G.2 Human resources security
- G.3 Physical and environmental security
- G.4 Access control to gaming systems
- G.5 Information systems security
- G.6 System availability and business continuity

Annex B (L Controls) Controls for the operation of games

- L.1 Physical instant tickets
- L.2 Lottery draws
- L.3 Retailer security
- L.4 Prize payment
- L.5 Payment methods and player accounts

L.6 Sports, esports, and horse race betting

L.7 Interactive Video Lottery Terminals (VLT)

L.8 Random Number Generation

L.9 Online games

L.10 Game design and approval

Annex C (S Controls) Controls for the development of gaming systems and the provision of gaming services

S.1 Gaming system security assurance

S.1.2 Integrity measures related to the development of gaming system hardware, software, and firmware

S.1.3 Integrity measures related to printing of physical instant tickets

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

M.1.2 Security of retailer point of sale device

M.1.3 Quick picks

M.1.4 Separation between ICS and CGS

M.1.5 Draw process

M.1.6 Intrusion detection system

Foreword

The World Lottery Association (WLA) is an international trade organization that represents state-sanctioned lotteries and betting operators, as well as suppliers of the global gaming industry. According to the WLA By-Laws, member lotteries and betting operators must be licensed or authorized to conduct lotteries or sports betting by the jurisdiction in which their gaming products are sold.

The WLASecurity and Risk Management Committee (SRMC) consists of representatives and security specialists from lottery and gaming operators, as well as other lottery professionals from around the world. SRMC members are duly appointed by the WLA Executive Committee. The WLA SRMC reviews the WLA Security ControlStandard (WLA-SCS) and is authorized to oversee the selection process of certification auditors, as well as to advise the WLA and its members on security and risk management issues.

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 aligned in accordance with the ISO/IEC 27001 standard.

Introduction

This document has been written by the WLA SRMC, incorporating relevant comments and feedback received by WLA-SCS auditors and WLA members.

The security and integrity of lottery and betting activities play a critical role in maintaining the public's confidence and trust in the sector. It is therefore vital that gaming operators, and gaming organizations in general, develop and maintain a visible and documented security and integrity environment to achieve and sustain public confidence in their operations.

With theCoP:2024 the WLA aims to support the understanding and the application ofWLA-SCS:2024 controls at a global level.

Scope

The CoP:2024 is designed to support:

- WLA members that are organizing their Information Security Management Systems in preparation for a WLA-SCS:2024assessment.
- *WLA-affiliated auditors conducting WLA-SCS:2024 assessments of WLA members.*

Some of the implementation guidelines shown within this document could be interpreted as extending the scope of the corresponding controls of the WLA-SCS:2024. In this case, the control provided by the implementation guidance should be considered as best practice only.

Normative references

The following documents are normatively referenced throughout CoP:2024 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 security, cybersecurity and privacy protection — 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:2024
- Guide to Certification for the WLA-SCS.

Terms and definitions

For the purposes of this document, the terms and definitions given in WLA-SCS:2024 apply.

Annex A (G Controls) Organizational controls

Applicability: G controls apply to gaming operators and gaming suppliers. All G controls are mandatory for organizations claiming conformity to the WLA-SCS.

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

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.

Implementation guidance

In order to ensure that senior management is sufficiently focused on security and integrity, an organization should establish a formal structure, a committee, or another equivalent group whose mandate is ensuring that security controls are effective and that security risks are being identified and managed appropriately. It is not the responsibility of the security forum to take ownership of security risks, but rather to ensure effective security risk management is in place.

Best practices would include making sure the membership of the security forum is sufficient to provide effective challenge on the strength of the security control environment.

There should also be adequate, cross-functional, wider business representation on the security forum.

Members of the security forum should be part of top management or report directly to top management.

For WLA-SCS level 1 certification, where an ISMS might not exist, the security forum should monitor and review the security control environment within the organization.

For organizations with an ISMS, the security forum could be used to help meet the management review requirements found in ISO/IEC 27001.

Examples of audit evidence

- Organization chart and reporting lines from the security forum to top management.
- Mandate / terms of reference of the security forum.
- Meeting minutes of security forum or management reviews.

G.1.1.2 - Security function

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.

Implementation guidance

The security function's role includes the development of a security strategy that aligns with both the wider business strategy and the security risk profile of the organization. Best practices would show the mapping between the security strategy and the security risk register to demonstrate how its delivery will help better manage risk over time. There might be one or more security strategies for different security domains (e.g., information security, personnel security, physical security) depending on how the organization is structured

It is also the responsibility of the security function to ensure that security is implemented in the business processes that are critical to the lottery and to ensure that the personnel have sufficient skills, training, and awareness about security. The security function should have the competence and resources to support the lottery and to minimize risks that could occur.

Examples of audit evidence

- Security strategy.
- Organization chart.
- Documentation describing the mandate / remit of the security function or scope of their authority.

G.1.1.3 - Security function reporting

The security function shall report to nolower than executive level management and shall be independent of thetechnology function with regard to the management of security risk

Implementation guidance

To ensure that the ISMS and security controls are well implemented, that risks are known and understood by top management, and that leadership of the organization actively considers security in their wider decision making, the security function shall report to and have regular interaction with

executive level management. Best practices will include regular formal reporting and discussions on security risk and security proactively involved in strategic discussions and decision making.

If the security function reports to the technology function, to avoid a conflict of interest between delivery / operations and security risk management, there should be a dotted line to another executive not responsible for project delivery, technology, or operations. This will ensure that security risk management decisions are not made by a single individual who might have conflicting responsibilities. Examples of appropriate dotted lines include, but are not limited to, the head of the internal audit function or head of the legal function.

Where the executive level manager is responsible for technology operations and / or project delivery, and is also responsible for security, then security is not considered independent of the technology function.

The security forum can be leveraged by the security function to assure independence from the technology function by having the security forum composed of senior managers representing the various sectors of the organization, beyond the technology sector.

Examples of audit evidence

- Organization chart.
- Job description of the head of security detailing their reporting line(s).
- Presentations given to the board or formal risk committee.

G.1.1.4 - Security function position

It shall have the competences and besufficiently empowered and shall have access to all necessary resources toenable the adequate assessment, management, and reduction of risk.

Implementation guidance

The security function should be adequately resourced with sufficient personnel and budget to discharge its responsibilities. The personnel responsible for security should be competent to fulfill the role and they should be evidenced by relevant qualifications, certifications, and previous experience.

Where security resources are deployed to other teams, or individuals have a significant security responsibility as part of their role, they should have a reporting line to the security function that allows the security function to effectively manage risk.

Examples of audit evidence

- Organization chart.
- Proof of the security personnel’s competence.
- Security budget.

G.1.1.5 - Security function responsibility

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

Implementation guidance

The head of the security function should proactively initiate discussions within the lottery and betting operations sectors on areas of security risk, where debate is required in helping obtain buy-in, resources, or investments pertaining to the management of security risk. Best practice would also see the head of the security function proactively recommending updates to security policies to ensure they align with both changes in threat as well as changes in business needs.

Examples of audit evidence

- Security forum charter / terms of reference.
- Security policy change log.
- Head of security job description.

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

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

Implementation guidance

The code of conduct gives the organization principles of good behavior among colleagues. It also often provides organizations with principles for reducing the risk of internal fraud or for preventing the misuse of information.

It should be noted that the code of conduct is applicable solely to employees. It is encouraged, when possible, to have the code of conduct, or an alternative version of it, applied to contractors or other third parties who work for the organization and, by virtue of their role or access, have the potential to impact the confidentiality, availability, or integrity of the organization's gaming systems, or alternatively place the critical elements of the code of conduct in the contractual agreements with these third parties.

Examples of audit evidence

- The code of conduct.
- Evidence of how updates are communicated to personnel.

- Evidence of acceptance of the code of conduct.

G.2.1.2 - Adherence and disciplinary action

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.

Implementation guidance

The reference to policies and procedures ensures employees are aware of their obligation to comply with them and provides a formal basis on which serious or repeated breaches of the code or the referenced policies and procedures can be dealt with.

Example of audit evidence

- The code of conduct section that covers possible disciplinary or similar action.

G.2.1.3 – Conflict of interest

The code of conduct shall include statements that employees are required to declare conflicts of interest in employment as and when they occur. Specific examples of conflict of interest shall be cited within the code.

Implementation guidance

Employees of the organization can have roles or commitments outside the organization. To ensure that the organization has all the necessary information about these external roles, employees should inform the organization of any possible conflicts of interest. An example of a conflict of interest would be when an employee of an organization with a technology function also has a role in, or owns shares in, the company of the developer of the independent control system (ICS).

Examples of audit evidence

- The code of conduct section that requires declarations to be made.
- A contractual agreement that requires such declarations to be made.

G.2.1.4 - Hospitality or gifts

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.

Implementation guidance

Gifts or hospitality from other companies or individuals can influence decision making. Best practice would be to oblige all employees to report any gifts or hospitality offered to them – whether accepted or not – and pose a maximum limit on the amount of any gift or hospitality that can be accepted.

Examples of audit evidence

- Code of conduct section that refers to hospitality and gifts.
- Gift and hospitality policy.
- Register(-s) in which gifts and hospitality over a stated value are recorded.
- A gift and hospitality register (record of gifts offered and given to others, as well as any gifts received or accepted by the organization).
- A register of disclosed gifts and hospitality.
- Notifications by employees to their line manager about any offered or received gifts/hospitality.
- A training program to provide staff with the tools to deal with dilemmas around the giving and accepting of gifts and hospitality.
- Employee surveys with questions that serve to clarify doubts and identify pressures on staff regarding hospitality or gifts.

G.2.1.5 – Corporate wagering policy

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 gaming operator or supplier itself).

Implementation guidance

Organizations should establish a policy that defines who can play games and who should be prohibited from doing so. The policy should recognize the risks associated with anyone affiliated with the lottery having a legitimate win, as it might create doubt on the game's integrity in the minds of others. Best practice would be to have a process to monitor both new accounts created with the gaming operator as well as any prize claims against those who are prohibited from playing, to ensure compliance with the policy.

The control applies to all parties that can potentially impact the integrity of a game, be it internal employees, contractors, or suppliers.

Suppliers’ policies should ensure all jurisdictions they support or operate in are covered by the policy.

Examples of audit evidence

- List of positions who are not allowed to play.
- Code of conduct with a section that covers this subject.
- Clause on the contract with the personnel stating if they are not allowed to play.
- Clause on the contract with the supplier/s stating they are not allowed to play.

- The corporate wagering policy.

G.2.1.6 – Personnel security

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 organization to protect the integrity of the games.

Implementation guidance

Organizations should have a vetting process for establishing who they are placing their trust in, before they do so, and through the life of the individual holding a sensitive role. Best practice would be to verify the identity of personnel to be assigned to sensitive roles, check for any criminal records, and ensure that individuals do not have any significant financial debt before holding a sensitive role.

Regarding monitoring activities, organizations should identify where there is risk to integrity. This might be anything from ensuring the integrity of a certain area of code, or a configuration file on the server, or access to a report on unclaimed prizes. For sensitive areas, a monitoring process should be in place to proactively alert any suspicious activity for investigation.

Examples of audit evidence

- Vetting policy and process.
- Examples of logs and rules to alert on behaviors that could impact game integrity.

G.2.1.7 – Segregation of duties

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.

Implementation guidance

There should not be a single individual (or team) that can impact game integrity without oversight. Best practice would be to look at all key processes (e.g., the conducting of the draw, the publishing of results, prize validation and payment) to ensure that there are no scenarios where an individual (or team) has sufficient access or authority to commit fraud.

Other examples include, but are not limited to, full separation of pre-production and production, and distribution teams in physical instants production, or separation between those that develop gaming systems and those that operate them.

For small organizations, where the implementation of this control could be more challenging, it might be useful to consider compensating controls.

Examples of audit evidence

- List of identified critical positions where collusion could occur.
- Segregation of the duty rules.

G.2.1.8 – Policy on employee protection

A policy shall be established to ensure that employee conducting lone working, those working remotely outside the organization's premises, or those working inside the organization's premises in areas with public access, are receiving an adequate level of protection with regard to both their safety and security.

Implementation guidance

Employees working outside the organization, or interacting with the public, could be exposed to threats or violence. To ensure that this risk is minimized the organization should provide adequate education, and if necessary, protection.

By way of example this could include the provision of, and the monitoring of. distress/panic alarms.

Examples of audit evidence

- Evidence of education provided to employees.
- Process for checking on staff who are conducting lone working.

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

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. The list of critical areas shall be documented.

Implementation guidance

Information assets should be physically protected to avoid or minimize the risk of damage or theft. Physical security best practices would include multiple layers of protection to prevent entry by

unauthorized individuals and detective controls such as CCTV and intrusion detection systems to deter and detect any attempted compromise.

When using cloud computing services or managed services in general, physical access to office spaces of the organization used by personnel to remotely access the production gaming system should be considered in the list of critical areas and protected according to identified risk.

Examples of audit evidence

- Automatic or manual log showing access to data center.
- Visitor log.
- Demonstration of video surveillance.
- Contract of job description for security personnel.
- Floor plans overlayed with physical security controls.

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 gaming suppliers G.4 controls shall be applied to the code repositories used to develop gaming systems.

G.4.1.1 - User access functions

The range of functions available to the user shall be defined and maintained in conjunction with the process owner, the IT function, and the security function.

Implementation guidance

Access to gaming systems should be allocated to users based on the principle of least privilege. Access should be consciously given to users based on their job role and revoked if they change the role or leave the organization. User access to gaming systems should be periodically audited according to the organization's access procedure.

Example of audit evidence

- Gaming system role-based access control matrix with permissions / functionality mapped to roles.
- User access audit files.

G.4.1.2 - User access logging

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.

Implementation guidance

The logging of critical events can be used to prevent or detect weakness in the access system of the gaming systems. The review of log events contributes to the reduction of this risk. Logs should be reviewed for all privileged accounts. For normal accounts, a risk-based approach would be sensible. Reviewing does not necessarily have to be manual. It could be automated using event correlation techniques to generate alerts for review. This control might extend to staging or pre-production environments as well as production if those environments could be used to impact game integrity.

Note: control **S.1.2.2** is about the system generating the logs and those developing the system ensuring adequate documentation so those logs can be understood by those charged with analyzing them. This control (G.4.1.2) is about undertaking reviews of the logs and acting upon them as appropriate.

Examples of audit evidence

- Log events and reports of the review process.
- Triggered alarms or incidents.

G.5 Information systems security

G.5.1 Cryptographic controls

Objective: To protect the confidentiality, authenticity, and integrity of cryptographic keys and important gaming 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 terminals

Cryptography to protect the confidentiality of information shall be applied for sensitive information on portable computer systems and to protect the integrity of sensitive information held at rest on terminals.

Implementation guidance

This control relates to the confidentiality and integrity of information at rest on a device such as a portable computer system (e.g., laptops, removable media, USB devices, and similar) and lottery terminals. Cryptography should be applied on sensitive information that risk analysis has shown to have an inadequate level of protection if left in its native form. Organizations should consider what information is stored on devices used outside secure locations and what the impact would be if that information were disclosed to those who are not authorized to see it or if unauthorized modifications were made to that information.

It is noted that some portable devices will not store data but process it only in volatile memory. In these cases, if the volatile memory is cleared then there is no requirement for additional cryptographic controls to be applied.

In cases where the storage used is immutable, then additional cryptographic controls for integrity are not required.

Cryptographic algorithms and key lengths should be in line with best practices.

Examples of information that risk analysis might determine requires additional cryptographic controls applied for confidentiality include details of prize claimants or unclaimed prizes held on a portable system.

Examples of information that risk analysis might determine requires additional cryptographic controls applied for integrity would include physical instant ticket game data moved onto a central gaming system using removable media, after having been received from a supplier of physical instant tickets. It might also include files that, if modified, could impact random number generation on a lottery terminal.

Example of audit evidence

- Group policy on a Windows/MAC system that enforces BitLocker or equal encryption on laptops and removable media.
- Tests showing data exported to removable media from a corporate device is automatically encrypted.
- Encrypted partitions on storage (if there is storage) within a lottery terminal (if sensitive lottery information is stored on the terminals).

G.5.1.2 - Cryptographic controls for the confidentiality and integrity of data in transit over networks

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.

Implementation guidance

This control relates to both the confidentiality and integrity of data while in transit. Cryptographic controls should be chosen to mitigate the specific risk (e.g., a cryptographic primitive designed to provide confidentiality will not necessarily protect integrity). Lotteries should ensure that data is protected as it passes across public networks, and they should assess the risk as to what is proportionate when data transits private or internal networks. Cryptographic algorithms and key lengths should be in line with best practices.

Examples of audit evidence

- Packet capture showing data is protected in transit.
- Configuration on a server / infrastructure showing appropriate use of cryptographic controls.
- Policy regarding the use of cryptography in network communications.
- Code showing integrity checks being conducted.

G.5.1.3 - Cryptographic controls for the integrity of sensitive ticket data

Cryptographic controls for integrity shall be applied for the storage of winning ticket data and validation information. This control applies to all game types.

Implementation guidance

There are several diverse ways to achieve this requirement. By way of example a lottery could use a hash function to check the integrity of validation information as it passes between a supplier of scratch cards and the lottery operator.

Example of audit evidence

- Procedure for integrity checks.

G.5.2 System testing

Objective: To enable and conduct system testing.

G.5.2.1 - Test methodology policy

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.

Implementation guidance

Test data is used to verify that changes or new lottery services are correct and secure. Test data samples could be created based on earlier gaming transactions prior to the current draw period. Another option might be to generate test data. Alternatively transforming production data in some way through methods such as zeroing out, masking or otherwise are possibilities but care should be taken here on the exact algorithms used for the transformation and which attributes in the overall data schema the transformation will be applied to. To reduce the risk of production data being stored and processed in a potentially less secure test environment, the lottery should have clear procedures showing how this risk is managed.

Examples of audit evidence

- Test procedure.
- Awareness training given to test personnel.

- Procedure for anonymizing sensitive data copied from production environments into test environments.

G.5.2.2 - Gaming system security testing

Thorough testing of the gaming system security functionality shall be performed prior to production environment use and on any significant changes.

Implementation guidance

Security testing can take different forms. Here below are some examples:

- Testing of security features and security functionality.
- Vulnerability testing.
- Penetration testing.
- Code review.

The type of testing conducted should be commensurate with the risk posed by the changes being introduced into the system.

Testing should follow a recognized methodology such as OSSTMM, OWASP®, or a similar methodology.

Testing should only be conducted by those with sufficient experience and competence. Those testing the change should be independent of those who have designed or developed the change, although they can reside in the same organization.

If the developer of the system and operator of the lottery are one in the same organization, then this control can be combined with the testing required in **S.1.1.3**. However, if the system is developed by a third-party supplier, then the supplier should ensure the product or service they are providing is secure (**S.1.1.3**) before it is passed across to the lottery, who should then perform their own security testing, if the change is considered as a significant change, as part of this control (G.5.2.2).

Examples of audit evidence

- Test plans.
- Test reports.
- System change log.

G.5.3 Managed services security

Objective: To ensure information security of gaming systems and gaming systems components managed by third parties or hosted in the cloud.

G.5.3.1 - ISO/IEC 27001 compliance

Managed environments (including cloud services, hosted services and in general managed services) that run gaming systems and gaming system components shall be compliant with ISO/IEC 27001. A managed environment is defined as computing resources managed by a third party and to which the organization subscribes to for services.

Implementation guidance

Any part of the gaming systems that are managed by a third party should be covered by a risk assessment and managed within the ISMS.

ISO/IEC 27001 certification is the easiest way to cover this requirement but in case the supplier is not ISO/IEC 27001 certified, the operator shall demonstrate that all the relevant controls of the ISO/IEC 27002 have been assessed and that there is a formal governance around risk management of those components.

Examples of audit evidence

- ISO/IEC 27001 certificate of the service provider.
- Attestation that the controls of the ISO/IEC 27001/27002 framework have been assessed by the service provider.
- For a cloud provider, ISO/IEC 27017: 2015 or more recent certificate.

G.5.3.2- Documented responsibilities and procedures

The following elements shall be documented, communicated, and implemented:

- Responsibilities for shared information security roles between the organization and the managed service provider.
- Procedures for administrative operations on the managed service environment and monitoring of these.
- A termination process that covers return and removal of the organization's assets in a timely manner.

Implementation guidance

When you outsource some of your operations or host your systems in the cloud the responsibility is shared with your service provider.

The operator must clearly identify the key assets and the operations so that controls can be defined, and adequate governance can be set.

The operator should define or extend its existing policies and procedures in accordance with its use of cloud services and make cloud service users aware of their roles and responsibilities in the use of the cloud service.

The operator should document procedures for critical operations where a failure can cause unrecoverable damage to assets in the cloud computing environment.

Examples of the critical operations are:

– installation, changes, and deletion of virtualized devices such as servers, networks, and storage.

– termination procedures for cloud service usage.

– backup and restoration.

The document should specify that a supervisor should monitor these operations.

The operator should request a documented description of the termination of the service process that covers return and removal of cloud service customers' assets followed by the deletion of all copies of those assets from the cloud service provider's systems

For cloud providers, ISO/IEC 27017 would cover this control.

Examples of audit evidence

- Shared responsibility matrix (RACI).
- Governance policy with the provider.
- SLAs and steering committees with the service provider.
- List of the assets.
- Schedule for the termination of service.
- Critical operations procedures.
- For a cloud provider, ISO/IEC 27017:2015 or more recent certificate.

G.5.3.3 - Segregation and access control

The managed service virtual environment of the organization shall be protected from other host service customers and unauthorized persons.

Implementation guidance

When outsourcing a service in the cloud, a risk analysis shall be performed to clearly identify how the data will be managed and to set controls to secure the service adequately.

The operator should verify that the cloud service provider enforces appropriate logical segregation of cloud service customer data, virtualized applications, operating systems, storage, and network for:

– the separation of resources used by cloud service customers in multi-tenant environments.

– the separation of the cloud service provider's internal administration from resources used by cloud service customers.

For cloud providers, ISO/IEC 27017 would cover this control.

Examples of audit evidence

- Technical architecture document.
- List of controls in place by the service provider and evidence that the controls are correctly set.
- SOC2 Type 2 report.
- For a cloud provider, ISO/IEC 27017:2015 or more recent certificate.

G.5.3.4 - Hardening and protection of virtual components

When configuring virtual machines or containers, gaming operators and cloud service providers should ensure that appropriate aspects are hardened (e.g., only those ports, protocols and services that are needed), and that the appropriate technical measures are in place (e.g., anti-malware, logging) for each virtual machine used.

For cloud providers, ISO/IEC 27017 would cover this control.

Examples of audit evidence

- Hardened master image.
- Hardening policy.
- For a cloud provider, ISO/IEC 27017:2015 or more recent certificate.

G.5.3.5 - Monitoring

The organization shall have the capability to monitor specified aspects of the operation of the managed service that the organization uses.

Implementation guidance

The operator should request information from the cloud service provider regarding the service monitoring capabilities available for each cloud service.

Examples of audit evidence

- List of access controls.
- List of SLAs.
- For a cloud provider, ISO/IEC 27017:2015 or more recent certificate.

G.5.4 Gaming system security

Objective: To protect the confidentiality, integrity, and availability of gaming systems in order to protect gaming and player data.

G.5.4.1 - Layered systems architecture

The organization shall provide a layered approach to security within the gaming systems architecture to ensure secure storage and processing of data.

Implementation guidance

Network aspects:

Network should be partitioned accordingly to these following principles:

- Different network areas should be defined according to the levels of sensitivity of the hosted assets and manipulated data. Assets that are exposed on the Internet shall be separated from other types of assets.
- A secure interconnection gateway (DMZ area) should be deployed to protect internal layers of the information system from Internet flows.
- The filtering equipment is implemented and monitors the inbound and outbound traffic of each area.
- The flows matrices are formalized and used as referential for the filtering equipment configuration. The matrices and configuration firewalls are periodically reviewed to detect inconsistencies or out-of-date parameters.
- Sensitive assets are not directly accessible from the Internet.

System aspects:

- Assets are classified according to the sensitivity of their roles within the infrastructure.
- Specific security measures are defined in relation to their classification.
- Systems are designed following the n-tiers models. A system should not have more than one responsibility.
- Systems with different levels of sensitivity cannot be hosted on the same physical infrastructure.
- Dedicated systems should be deployed for administrative operations. Mutualization with less sensitive operations should be forbidden.

Examples of audit evidence

- Functional Architecture document.
- Technical Architecture document.
- A list of all the system’s IT components with their classification.

G.5.4.2 - Responsible disclosure

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

Implementation guidance

There should be a policy and an associated process for dealing with responsible disclosures. This should identify where reports should be made, if necessary, and how rapidly they will be assessed and acted upon.

Best practice would be to include a security.txt file on all gaming operator branded, Internet-facing websites.

Example of audit evidence

- Responsible disclosure policy.

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

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 games, as well as the availability and resilience requirements of those services. Systems shall be architected to meet those requirements.

Implementation guidance

Availability requirements are often used to measure fulfillment of security objectives, but also enable capacity planning and disaster recovery prioritization. Identifying and documenting critical services to players gives the organization a better overview for monitoring and incident handling. Critical services should therefore be classified according to how critical each service is to the player. Organizations should have a procedure in place to control the critical services when these are changed, or new services are established.

Availability requirements to critical services should be formally approved by the security forum and board of directors, taking into consideration stakeholder's expectations, and include both requirements in a normal operation and a disaster recovery operation. Organizations should undertake a risks evaluation to ensure that the organization's requirement is considered.

By articulating availability requirements an organization can settle the cost versus risk tradeoff about architecting resilience and redundancy into their systems.

Examples of audit evidence

- List of systems showing availability and criticality requirements.
- Monitoring reports on present availability.
- Procedures on how critical services are classified.
- Availability requirements decision given by the security forum.
- Risk evaluation reports.

G.6.1.2 - Business Continuity

The organization shall prepare a documented business continuity plan that covers, at minimum, the continued operation of games and continued stakeholder confidence in the integrity of gaming 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.

Implementation guidance

Organizations should have a resilience plan to ensure that critical services can be provided in a crisis or disaster situation. Continuity planning should cover the range of realistic events that could impact the organization such as, but not limited to, pandemics, loss of the availability of key systems for a significant period, or natural disasters.

Exercises should be conducted with different individuals and teams in the organization and should take different forms. This could involve physically moving a team to operate out of a business continuity site, running a tabletop exercise, or switching off systems to test automatic failover to other systems in the cluster.

ISO 22301 provides good guidance and advice on crisis management but is not required to be used during the WLA SCS audit.

Examples of audit evidence

- Business continuity plan.
- Action plan on when to do exercises.
- Audit reports.
- Evidence that exercises have been executed on critical systems.
- Learning reports from conducted exercises (i.e., workshop exercises).

Annex B (L Controls) Controls for the operation of games

Applicability: L controls apply to gaming operators. Applicable L controls are mandatory for gaming operators claiming conformity to the WLA-SCS.

L.1 Physical instant tickets

L.1.1 Instant game operations

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 - Lifecycle management and integrity requirements

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.

Implementation guidance

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.

There are many security aspects to take into consideration when designing and producing instant games. These include conforming to applicable laws; avoiding controversial game motifs (political, social, religious); identifying errors in game rules or prize structures; identifying errors during the production, distribution, and disposal of tickets; and, preventing fraud.

Formal procedures that cover the entire instant game lifecycle, and contain integrity requirements for each instant game, should be established. Integrity requirements to take into consideration are:

- Visuals and texts:
  - Compliance with current legislation, copyright.
  - Conduct of a social impact analysis (controversial visuals, responsible gaming).
  - Validation of game rules, visuals, and texts printed on tickets (comprehension, respect for game rules).

- Quality controls. The scope ofquality controls should include, but not be limited to the following areas:
  - Programming
    - Compliance with game mechanics.
    - Compliance with prizestructure.
    - Compliance with specificationsfor the distribution of tickets in the books (Guaranteed Low End PrizeStructure – GLEPS), if applicable.
  - Printing
    - Non-predictability of aticket's winning status based on visible information.
    - Ticket opacity tests: Usingvarious techniques to determine whether a ticket is a winning ticket withoutscratching it or without visibly altering it.

- Tests
  - Internal quality and security tests (by the printer).
  - L.1 Physical instant tickets
  - L.1.1 Instant game operations

- Protection of validation/winner files.
  - Encrypted validation numbers.
  - Encrypted validation and winner files.

- Inventory
  The lottery operator should be able to follow instant ticket stocks to detect any loss/theft. Here are examples of actions that could be taken in this area:
  - Inventory of available ticket books in a lottery's facilities.
  - Inventory of tickets to be destroyed.
  - Monitoring of retailer stocks.
  - Monitoring of instant tickets in transit.
  - Investigation of book loss and reporting to security function as appropriate.

Examples of audit evidence

- A documented procedure, covering the entire game lifecycle that describes integrity and test requirements implemented by the organization.
- Evidence of the controls applied by the operator.

L.1.1.2 - Game data integrity

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.

Implementation guidance

To prevent errors and fraud, the lottery operator should implement controls that mitigate risks to the game-data integrity. Ideally, those controls should be documented in the procedure mentioned in **L.1.1.1.** Here are some examples of controls to take into consideration:

- Implement encryption measures to guarantee the integrity and the confidentiality of game data during its transfer from the printer to the lottery system.
- Give access to the gaming system on a least privileged basis.
- Provide appropriate security awareness to personnel with access to the gaming system.
- Ensure the integrity of the instant game data loading into gaming systems through the following measures:
- Implement checklists to ensure that all controls are executed.
- Test the loading of game data on test systems.
- Use the four-eyes control principle to load the game data and check that imported game data matches the expected instant game.

Examples of audit evidence

- A documented procedure describing the controls developed by the lottery operator.
- A procedure, agreed upon with the printer/supplier, which describes security requirements for game data that is transferred to the lottery operator.
- Evidence of the controls applied by the lottery.

L.1.1.3 - Ticket prize confidentiality

Controls shall be in place to ensure that prior to the claiming of a prize no one in the organization has access to 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.

Implementation guidance

The printer/supplier can determine which ticket is winning or not. On the other hand, the lottery operator has knowledge of where the books of tickets are located. To prevent fraud, the lottery operator should ensure that no one has the knowledge of both where the books of tickets are located, and which tickets are winning tickets. Here are some best practices that can be applied:

- Any requirements to the printer regarding the confidentiality of validation data (e.g., contract, audit result, certification covering the control S.1.3.2.3 of the WLA-SCS:2020).
- A written process describing ticket reconstruction requests.
- Lists of reconstruction requests.

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

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.

Implementation guidance

A global policy should be defined that documents the guiding principle of lottery draws and the publication of results. For both, the following principles should be identified:

- The general organization of a draw: the role and duties of the individual draw internal participants, the required documentation, the management planning.
- The accredited external participants: the security officer, the court bailiff/regulator representative (depending on applicable regulations).
- The physical security measures in place to protect both processes: video camera, access control, guards.
- The possible draw locations/sites/rooms should be identified: this also includes the location(s) used for announcing the results.
- Physical resource management: lottery ball set, draw machine.

Examples of audit evidence

- Draw policy.

L.2.1.2 - Draw working instructions

The organization shall publish a working instruction prior to any draw including special instructions with respect to the draw.

Implementation guidance

Operational procedures detailing the entire drawing process – before, during, and after should be formalized. The operational procedures should be defined for each type of game.

Each type of game includes:

- The different steps for each range of the game. The description of each step should answer the question: Who does what, when, where, why, and how to do it?

- The different (internal and external) participants, along with their roles and duties.
- The different physical resources.
- The different activities to perform and their results.
- The sequencing of these activities.
- For each draw location and for each range of the game, the role of the observers / external participants should be defined. Their roles and duties (before, during, and after) a draw should be specified.
- The list of draw managers for each game.
- The draw managers schedule for each game, as evidence that their appointment has been published.
- The list of staff members and internal contacts with their functions, internal phone number, mobile phone.

Examples of audit evidence

- Operational procedures.
- Working instructions issued before any draw.

L.2.1.3 - Draw team members

The working instruction shall include the composition of a draw team including their contact telephone numbers.

Implementation guidance

See the implementation guidance of controls **L.2.1.1** and **L.2.1.2**.

Examples of audit evidence

- See the examples of audit evidence of controls **L.2.1.1** and **L.2.1.2**.

L.2.1.4 - Draw team duties

The working instruction shall include the duties of the identified members of the draw team.

Implementation guidance

See the implementation guidance of controls **L.2.1.1** and **L.2.1.2**.

Examples of audit evidence

- See the examples of audit evidence of controls **L.2.1.1** and **L.2.1.2**.

L.2.1.5 - Reserve draw team

The working instruction shall nominate persons as reserves and detail how the reserve team are deployed.

Implementation guidance

See the implementation guidance of controls **L.2.1.1** and **L.2.1.2**.

Examples of audit evidence

- See the examples of audit evidence of controls **L.2.1.1** and **L.2.1.2**.

L.2.1.6 - Draw timing

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.

Implementation guidance

See the implementation guidance of controls **L.2.1.1** and **L.2.1.2.**

Examples of audit evidence

- See the examples of audit evidence of controls **L.2.1.1** and **L.2.1.2**.

L.2.1.7 - Draw observers

The working instruction shall include details of any requirement under the lottery rules for independent observers to be present during a draw.

Implementation guidance

See the implementation guidance of controls **L.2.1.1** and **L.2.1.2**.

Examples of audit evidence

- See the examples of audit evidence of controls **L.2.1.1** and **L.2.1.2**.

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

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.

Implementation guidance

To complement the operational procedures mentioned under section **L.2.1**., a control check list should be specified for each main function in the draw process, by type of game.

Examples of audit evidence

- Operational procedures.

L.2.2.2 - Draw step-by-step guide

The draw procedure shall include a step-by-step guide of the draw process.

Implementation guidance

(See section **L.2.1**)

The operational procedures should be formalized and detail each step of the draw process (before, during and after) as well as the announcement of the draw results.

For the draw process, the following steps should be described:

- The draw preparation and practice step: The individual responsible for each action, the material required, the deadline for each action, and the control actions should all be identified.
- The draw step: The individual responsible for each action, the material required, the deadline for each action, and the control actions should all be identified.
- The announcement of the draw results (see below).
- The storage step of the draw appliance(s) and material: The individual responsible for each action, the material required, the deadline for each action, and the control actions should all be identified.

For the process of announcing the draw results in each range of the game, the steps should specify the following:

- The list of official media communicating the results including: the names of the entities, the file format forwarded to these entities, the deadlines for sending, and the means of sending (e.g., email, internet site).
- The possible controls before announcing the results: the different means for checking (i.e., PC – desktop or laptop), what are the check points, who oversees the checks.
- Recording the results: when the different actions should be done, who are the accredited and mandatory participants (internal and external), and what is the check point.
- The approval of winnings: The winning calculation method should be specified for each range of the game.
- Depending on the game (i.e., EuroMillions), the winners' approval should also be defined: The count and the check of winners.

- Result sending: What is the publication workflow? Indicate when the different steps of this publication should be taken; Who are the accredited and mandatory participants (internal and external); What are the check points? What are the possible media for the publication?

Examples of audit evidence

- Draw policy.
- Operational procedures.
- Working instructions issued before any draws.

L.2.2.3 - Draw location

The draw procedure shall include the definition of the draw location.

Implementation guidance

For each game, the different draw locations should be identified.

To complement the above operational procedures (see **L.2.1)**. The following information should be specified:

- The different security measures should be defined for each location/site/room.
- The process of accessing the draw location/site/room should defined: type of access control (i.e., biometric), identification of people who have access to each location/site/room.
- The internal phone numbers of possible draw locations should be identified and communicated to internal stakeholders: i.e., the guard post, on-call staff.
- Backup draw locations should be identified in case of an incident at the primary location. The following should be defined for each game:
- The details of the draw and the activities of the announcement of the results.
- The identification of each required participant.
- The material necessary for the draw and for the announced results.

Examples of audit evidence

- Draw policy.
- Operational procedures.
- Working instructions issued before any draw.

L.2.2.4 - Draw attendance and responsibilities

The draw procedure shall include a definition of the attendance at the draw and the responsibilities and actions of all participants.

Implementation guidance

To complement the above operational procedures mentioned under **L.2.2.1**, and **L.2.2.2**, where all attendees with their responsibilities are defined, the following information for each game should be specified:

- The list and schedule of draw managers: The name of the draw manager with their phone number, their function, the date or intervention period, and the game.
- The list and schedule of staff members: The name of the staff member, the date or intervention period, and their function.

Examples of audit evidence

- Draw policy.
- Operational procedures.
- Working instructions issued before any draw.

L.2.2.5 - Draw supervision

The draw procedure shall define the policy regarding the attendance of an (independent) compliance officer or an auditor.

Implementation guidance

To complement the above operational procedures mentioned under **L.2.2.1**, and **L.2.2.2**, where all attendees with their responsibilities are defined, the following information for each game should be specified:

- The identification of compliance officer (for example the Draw Marshall) should be specified: Specify the scope and purpose of their game intervention.
- The list and schedule of possible official independent officers (for example the bailiff depending on the local regulation): List their name, their organization, and the date or intervention period.
- A procedure of “official independent officers” missions should be defined: the operation scope for the game, the requirements, the schedule, the incident management (process incident, lack or delay of the officer, material incident).

Examples of audit evidence

- Draw policy.
- Operational procedures.
- Working instructions issued before any draw.

L.2.2.6 - Draw operation security

The draw procedure shall include adequate security measures for the draw operation and all equipment used during the draw process.

Implementation guidance

To complement the above operational procedures mentioned under **L.2.1**, the following information should be specified:

- The specification of security service: The scope and purposes of their intervention for each game, the description of security service office.
- The description of the premises, access and equipment for the draw should be specified: location, access control and access rights (identification of the groups that have access to the location).
- The specification of possible different rooms (i.e., equipment storage room, room for the announcement of results, safe room): location and use, their access control and access rights, the security measures (for example CCTV).
- Description of the draw equipment and how it works. This includes the description and use of the draw equipment, the description, and the use of the balls for each draw, where applicable.
- Controls should be set to check the operational procedures.

Examples of audit evidence

- Draw policy.
- Operational procedures.
- Working instructions issued before any draw.

L.2.2.7 - Draw emergency

The draw procedure shall include actions in the event of an emergency occurring at any time during the course of the draw.

Implementation guidance

To complement the above operational procedures mentioned under **L.2.1**, procedures for emergencies or incidents should be specified for each game. These procedures encompass the incident classification and their treatment modes for the draw process and declaration of the results.

- The definition of blocking (and non-blocking) incidents and who is in charge of managing such incidents.
- The incident management process:
- Who is in charge of declaring the incident?
- How the incident should be declared: A message with the required information (the sequence of operations, the timing and duration of any interruptions, delays, or other disruptions.
- The incident communication process towards interested parties (players, media.).
- The treatment of an incident that occurs (before, during, or after) the draw or the declaration of results: Depending on the nature of an incident (human, material, or IT) a detailed action plan

should be specified with the owner of each action.

Examples of audit evidence

- Draw policy.
- Operational procedures.
- Working instructions issued before any draw.

L.2.2.8 - Draw integrity, alerting and reporting

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.

Implementation guidance

To complement the above operational procedures mentioned under **L.2.1**, procedures on draw integrity should be specified for each game (some controls may be standardized). These procedures encompass the access, the monitoring, and the alerting of the gaming system.

Examples of audit evidence

- Periodic access reports.
- Suspicious activity alerts.
- Periodic activity monitoring.
- Design detailing the implementation of an independent control system

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

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.

Implementation guidance

Technical specifications and standards should be defined (e.g., weight, diameter, bounce, radiography for the ball sets) and communicated to a competent independent authority. The independent authority can be a standardization association member of ISO or a state accredited equivalent.

This authority should inspect the components in accordance with the specifications.

- The inspection frequency should be described.
- The response to the findings should be defined.
- In any case, components affected by inspection findings should not be used.

Example of audit evidence

- Independent authority report.

L.2.3.2 - Regular inspection and maintenance

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.

Implementation guidance

A maintenance procedure should be defined that details the actions done for:

- The level of maintenance:
- Repairing (curative or remedial actions).
- Tuning (preventive actions).
- Checking.
- The means of realizing the maintenance (internally and/or externally) should be identified.
- The details of each maintenance level should be specified.
- The traceability of each maintenance intervention should be defined.

A global planning for draw equipment maintenance should be available.

Example of audit evidence

- Inspection reports.

L.2.3.3 - Compatible ball sets

The organization shall establish a procedure that provides for the use of ball sets manufactured to those measurements and weight tolerances compatible with the drawing machine to be used.

Implementation guidance

A document should specify the tolerances and nominal values:

- The maximum and minimum allowable value of a ball diameter and weight.
- The nominal diameter and weight.
- The allowable maximum average spread.
- The maximum allowable spread.

- The average percentage of the spread.

The calculation and measurement methods should be specified.

Example of audit evidence

- Technical procedure.

L.2.3.4 - Replacement draw appliance

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

Implementation guidance

To complement the above operational procedures for the incident part (mentioned under **L.2.2.7**) and for the maintenance part (mentioned under **L.2.3.2**), a procedure should define the permutation policy of each draw appliance type, in each range of game (frequency and planning should be identified).

Example of audit evidence

- Technical procedure.

L.2.3.5 - Draw appliance and ball set handling, storage, and movement

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

Implementation guidance

To complement the above operational procedures for the incident part (mentioned under **L.2.2.7**), for the draw security (mentioned under **L.2.2.6**), and for the maintenance part (mentioned under **L.2.3.2**), the procedure should define:

- The type of draw appliances and ball sets and the number of appliances and balls sets that are available in each storage location.
- For each handling /movement, the actions should detail:
- Who is (are) authorized to handle draw appliance(s) / ball set(s).
- What is (are) the control(s) to perform (before, during and/or after).

Example of audit evidence

- Technical procedure.

L.2.3.6 - Broadcast / streaming of the draw

When the draw is broadcast or live streamed over the Internet, there shall be a procedure in place that minimizes the risks associated with data corruption, time 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.

Implementation guidance

To complement the above operational step by step procedures for the draw (mentioned under **L.2.2.2**), the following should be encompassed and defined:

- The rehearsal of the draws in broadcast configuration.
- The broadcast after the official draw.
- The actions to carry out, in case, for any problem.

It should be noted that a draw can either be broadcast (on TV channels, live or after the draw) or streamed live to the internet.

Example of audit evidence

- Technical procedure.

L.3 Retailer security

L.3.1 Retailer operations

Objective: To ensure that retailer operations, whether on or offline, conform to the organization's security requirements.

L.3.1.1 - Retailer security

The organization shall specify the obligations of a retailer and the security environment the retailer is required to operate in within an agreed contract.

Implementation guidance

There should be a valid contract between each point of sale (or chain of retailers) and the organization. The contract should include aspects related to the security conditions of the premises, the access procedure, and the operation of the gaming terminal (for the cases that apply). For example, the protection of access credentials, verification of the identity of the technicians who conduct maintenance, the identification of the point of sale.

It is customary to have a contract signed by the parties involved or their representatives.

One way to verify the identity of the maintenance technicians would be through the use of an exclusive mobile app for authorized points of sale that reads an existing code on the technician's identification card. This also serves to obtain information regarding service times.

Examples of audit evidence

- A contract signed by authorized persons.
- A control sheet of technicians authorized to attend the premises and periodic review of said authorization.

L.3.2 Gaming terminal security

Objective: To ensure the adequacy of the gaming terminal security.

L.3.2.1 - Transaction security

The data traffic between the gaming terminals and the central gaming system shall be protected and measures to ensure the integrity of the transactions shall be implemented. Where a retailer point of sale device is used instead of a dedicated gaming terminal, the data traffic from the gaming 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 games.

Implementation guidance

In the case of a dedicated gaming terminal, the manufacturer should provide technical information indicating how the integrity of the data between the application running on the terminal and the central gaming system is ensured.

Information classified as sensitive (e.g., personal data, options chosen, amounts wagered, i.e.) should always travel encrypted.

In cases where the terminal is not specific to the game (e.g., general POS or Smartphone), the application itself should be responsible for ensuring integrity and / or encrypting the information when appropriate.

One way to ensure integrity could be to apply checksums generated from hash functions that ensure the data was not modified.

At the network level, private communication networks should be used, or failing that, virtual private networks should be used if public networks are used. However, the use of public networks is not recommended.

Mechanisms with documented procedures should be established in the case of terminal replacement due to technical failure or other reasons. This mechanism should ensure that the new terminal is valid and corresponds to that sales location.

Note that if the retailer has an independent communication device, it would not be enough for the data protection (integrity and / or encryption) to be carried out at this point. In this way, the encryption provided by virtual private networks would not be sufficient since there would be a

section (between the application and the communication device) where the data would travel without protection.

Examples of audit evidence

- The manufacturer's technical specification indicates how to ensure the integrity of the information for dedicated terminals.
- The audit record of the transaction to verify the encryption of sensitive data.
- A procedure for the replacement or modification of point-of-sale equipment.

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

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.

Implementation guidance

The defined procedures could cover the generation of the winning transactions through their validation mechanism at the time the bettor claims a prize.

To generate the winning transactions, the systems in charge of the task must have a mechanism to ensure their integrity.

One way to ensure integrity is to include in the ticket data a hash with an electronic signature of the system responsible for generating the prizes.

In the validation procedure, it should be indicated what the bettor should do to validate a ticket and what information should be checked to verify that the ticket is correct.

The unique ticket reference identifier in **L.4.1.2** could be used to identify the ticket.

To authenticate the tickets, secret validation codes and hash codes can be used in addition to other special characteristics of the paper itself.

The validation procedure should consider all sales channels and all prize levels.

The expected hit rate (count and amount), prize plan, or prize level should be controlled for each game mode and for the game in general. A periodic report could be implemented with the results of

the control.

For games with fixed prize plans, a check should be made to ensure that each of the winners corresponds to the correct prize.

Checking random samples of generated winning transactions and making parallel settlements could be good practice, but this is not mandatory for ensuring proper operation.

Examples of audit evidence

- Validation procedures for each game.
- A parallel settlement log.
- An audit log of the sampling mechanism.
- Periodic reports on expected hit rate and prize levels for each game.
- A log of changes for settlement algorithm.

L.4.1.2 - Unique ticket reference

Each ticket for each game shall have a unique reference number.

Implementation guidance

An example for ensuring a unique number could be a code that includes the date of the day or timestamp, a game identifier, an identifier of the point of sale or terminal, and a sequential correlative for that point of sale.

As it is a finite code, it is necessary to make sure that this code complies with the necessary length so as not to repeat itself within a reasonable cycle.

The uniqueness of the tickets should be for both physical tickets and e-tickets.

Examples of audit evidence

- Document with the specifications of how each ticket is identified.
- Check a sample for real tickets.

L.4.1.3 - Security of unclaimed prize data

The organization shall implement technical and procedural controls to ensure the confidentiality, integrity, and availability of unclaimed prize data. This includes as a minimum, but is not limited to, 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.

Implementation guidance

An example of one possible way to protect the information of unclaimed prizes is to use a unique code to identify the transaction (see **L.4.1.2** control), a secret code – generated randomly – in addition to the information of the transaction itself, such as: the place where the transaction was carried out, the date and time of the transaction, the chosen options, the amount bet, etc.

This secret code should be long enough to prevent brute force attacks and printed on the ticket but never stored. The result of applying a cryptographic hash function (CHF) to all information (including the secret code) should be stored and should not be the secret code itself.

The objective is to make it impossible to completely reconstruct all the information in a ticket, since no one would know the secret code except the person who has the winning ticket.

If for any reason the information that allows the ticket to be reconstructed needs to be stored, that information should be encrypted using robust algorithms and strictly protected.

An example of the procedure for verifying a winning ticket could include the verification of the identity of the ticket (see **L.4.1.2**) together with the verification of the secret code of the ticket. Both codes could be part of a barcode to facilitate reading and avoid typing errors.

Access to information on winning transactions should be strictly audited and controlled and there should be a registry with the people who can access it.

Examples of audit evidence

- A formal procedure, including technical specifications, for validating tickets.
- Sample for real tickets.
- An updated record of the people authorized to access this information along with the history of changes.
- A log of access to unclaimed prize information.

L.4.1.4 - Prize payout procedure

There shall be a prize payout procedure that defines a maximum prize claim period; includes a process to audit final transfers upon game settlement; details the rules and due diligence required prior to making a decision on payout for a lost, stolen or damaged ticket; details the procedure with regard to inquiries into the validity of claims; and a procedure with regard to late or last minute payouts.

Implementation guidance

The payment procedure should clearly establish the claim period (e.g., a one-month period specifying whether the payment period starts from the date of the bet or from the date of the draw or event). In general, this period is part of the legal requirements of the organization and could be communicated on the back of the ticket itself.

For digital channels, you should specify whether user action is required or if the prize will be automatically credited. It is also important to establish if the organization has a different payment procedure depending on the award amount or the claim period (e.g., big prizes or late claims).

This payment procedure should meet all legal obligations that the organization has regarding tax applications or withholdings on the wins.

It is important to specify the conditions for a ticket to be considered valid. Tickets with damaged or illegible barcodes or identification codes should be considered invalid. The terms of the claim period should also be specified.

Authentication mechanisms related to watermarks, paper controls, or other similar mechanisms could also be valid.

Examples of audit evidence

- An approved document with specification of the aforementioned points (e.g., deadlines, stolen, lost or damaged ticket).
- A section or paragraph of the document where the terms of payment are specified.
- A section or paragraph of the document dedicated to lost or stolen ticket claims.
- A section or paragraph of the document that specifies when a damaged ticket is still valid for collection. For example: The legibility of the identification and authentication codes; that the damaged area is not greater than a certain percentage; that the ticket has not been repaired, altered, or manipulated.
- A section or paragraph on payment procedures according to the amount of wins.
- A section or paragraph of the documents where the taxes or withholdings on the wins are indicated.

L.4.1.5 - Fraud detection

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 that might require investigation.

Implementation guidance

This control could be implemented through automated systems that look for patterns or behaviors deviating from the average. To do this, artificial intelligence techniques or automatic learning applied to data mining could be used.

Examples of patterns to detect could be those of customers who play through digital media that have a higher-than-expected win rate, points of sale that collect a lot of prizes in percentage terms, or the late collection of prizes. As this is an automatic procedure, it can be applied to all wins. The system should record each execution and the findings be made available.

Another way would be to implement a random manual audit based on a sample with a special focus on the wins collected near the expiration period. The selection of the sample and the periodicity of the control should be representative of the number of wins.

There should be a process dealing with the escalation of incidents or suspicious activity.

Examples of audit evidence

- A formal procedure that includes the technical specification and cases covered.
- An audit log for fraud detection process.
- A log of changes for the fraud detection algorithm.

L.4.1.6 - Prize payout percentage monitoring

Games shall be monitored concerning security and prize payout percentage.

Implementation guidance

The objective of this control is to detect possible errors in the games and/or internal or external fraud related to the prize payout percentage of non-prefixed structure games and could be monitored for prefixed prize structure games based on risks.

The control should be verified that the prize payout percentage of a game is within its theoretical specification with a certain margin of tolerance.

One strategy is to carry out a global control at the level of the entire game and then control more specifically by variant or modality, sales channel, point of sale or even the client if it is identified.

To carry out more specific controls, it may be necessary to extend the study period to have a representative volume of data.

To ensure its effectiveness, the control must be carried out on a periodic, automated basis and have a formal procedure to handle deviations outside the tolerance margin.

When detecting a deviation above the tolerable margin in instant resolution games, one option is to pause the game until the cause is analyzed in detail.

It should be considered that the deviation can occur both in the payout and in the frequency of occurrence of prizes.

Examples of audit evidence

- Evidence on the control on the prize payout.
- Deviation handling procedure.

L.4.1.7 - Dispute or protest resolution procedure

There shall be documented procedures to handle dispute or protest from customer regarding a win or loss.

Implementation guidance

When an incident related to game occurs, the customer might want to claim a prize or dispute a loss.

The dispute or protest process should be easily available to the customer so that the dispute can be handled in a proper manner.

To ensure that cases are handled consistently, the dispute procedure should describe how this is ensured.

Examples of audit evidence

- Procedure that describes the dispute or protest process.
- Examples of protest handling.

L.5 Payment methods and player accounts

L.5.1 Securing payment methods

Objective: To protect payments methods against fraudulent uses.

L.5.1.1 - Data collection

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

Implementation guidance

The gaming operator should consider what data is strictly needed for the transaction and only that data should be collected. Taking into consideration the local regulations and laws, and the risk of identity theft.

Example of audit evidence

- PCI DSS certificate

L.5.1.2 - Payment method protection

Adequate measures shall be taken in order to protect any type of payment used in the system from fraudulent use.

Implementation guidance

The organization should refer to international standards, such as the PCI-Data Security Standard norm, which defines standards of data security in electronic payment processes for credit and debit

cards (recognizing that other payment methods might be supported by the lottery).

All information transmitted during payment should be secured by state-of-the-art encryption.

Former and unsecured suites of protocol should be refused by servers.

Example of audit evidence

- Specifications of controls and measures in place for payment protection.

L.5.1.3 - Payment service approval

The organization shall verify that the payment service ensures the protection of the player data, including any personally identifiable information given by the player or payment related data.

Implementation guidance

The confidentiality and integrity of information exchanged during the payment process should be guaranteed (refer to L.5.4.2 Payment method protection).

When a lottery operator delegates the hosting of payment services to a business provider, it should ensure that its contractual commitments, in matters of player data protection, are compliant with local laws and regulations as well as lottery operator policies (i.e. PCI DSS certificates).

Examples of audit evidence

- PCI DSS certificate of the payment service provider.
- Specifications of controls and measures in place for player data protection.

L.5.2 Player account

Objective: To protect the player and to manage the risk of fraudand money laundering in gaming systems requiring identified players.

L.5.2.1 - Player account

There shall be a formal process for identification, authentication, and authorization of a player. Both player data and the wallet shall be considered as critical assets for the purposes of risk assessment.

Implementation guidance

- Sensitive operations on critical assets should be subject to prior authentication.
- Segregation between different user spaces should be ensured.

Examples of audit evidence

- Procedures for the identification, authentication, and authorization of players.

L.5.2.2 - Multiple player accounts

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

Implementation guidance

Each user should only be identified by information that is known to be unique (e.g., an email address).

In accordance with the locally applicable laws, player identity information should be requested and verified before they can be allowed to play. Lottery operators should maintain a list of all player identities in order to verify that the identity of a player for the creation of a new account has not already been used.

Examples of audit evidence

- Procedures for identification, authentication, and authorization of players.

L.5.2.3 - Player exclusion

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

Implementation guidance

The rights, the duties, and the sanctioning of players should be established in accordance with local applicable laws and/or internal procedures and recorded in a document. The lottery operator should ensure that players understand, and agree with, this document in order to use the lottery's games and services.

Depending on local applicable laws, the organization should establish a procedure for managing available money stored in the wallet of an excluded player.

Pending payment transactions or game actions related to an excluded account should be identified and if necessary, stopped.

Depending on the context of the exclusion, an organization should establish procedures to manage the deactivation or suspension of the excluded player's account, on the concerned offer or on all perameters of gaming offers.

Example of audit evidence

- Procedures for identification, authentication, and authorization of players.

L.5.2.4 - Multiple payment instrument holder

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 to avoid fraud and money laundering.

Implementation guidance

Depending on local applicable laws, consistency of payment methods should be assessed before allowing any interaction with gaming functionalities (i.e., the identity on a player's civil status document should correspond to the identity of payment method identity).

Anonymous payment methods should not be accepted to prevent fraud.

Example of audit evidence

- Procedures for identification, authentication, and authorization of players.

L.5.2.5 - Transactional records related to payments

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

Implementation guidance

Each operation related to a transaction should be identified and logged in accordance with logging policy.

The transactional records should not contain secret information about player payments.

The integrity of the transactional records logs should be protected through cryptographical measures.

The storage of transactional records should be integrated into a secure backup process to prevent loss or unwanted modification.

Transactional records shall contain a unique key throughout its lifecycle.

The access to transactional records should be secured and restrict on a need-to-know basis.

Examples of audit evidence

- Logs of the transactional records.
- Operational procedures for the control of logs that trace the transaction lifecycle.
- Measures to secure the logs.

L.6 Sports, esports, and horse race betting

Definitions

The following definitions have been identified to clarify doubts around common terms used in the framework of sports betting activities, to create a common ground for action and enhance understanding.

Odds

In gambling, the odds-on display does not represent the true chances that the event will, or will not occur, but are the amount that the company will pay out on a winning bet, together with the required stake. In formulating the odds to display, the bookmaker will have included a profit margin, which in effect means that the payout to a successful player is less than that represented by the true chance of the event occurring. There are three major formats for odds that are: the decimal format (used in Europe), the fractional format (used in UK) and the American format. Here is an example of a table conversion between those formats:

Decimal	Fractional	American
1.50	½	-200
2.00	Even (1/1)	+100
2.50	6/4	+150
3.00	2/1	+200

Asian Handicap

Asian handicap is the most popular market among Asian betting markets. As football matches often involve draw results, the introduction of Asian handicap helps to eliminate the possibilities of the draw result, and the possibilities are spread onto Home and Away selection. A more balanced betting environment is created as a handicap, expressed in terms of goals, is put into effect onto the favorites to make the chance of either selection as close to 50% as possible. The handicaps are given in quarters (0.25). And bets on the .25 and .75 selection would be evenly spread onto 0/0.5 and 0.5/1.0 respectively.

The market Asian Handicap has eliminated the draw selection and is solely a two-way market. Which suits a lot of the punters well, as they can relate the Asian Handicap to the two-way betting markets they would see in American Football, Basketball or Tennis. The difference between the “European Handicap” and the Asian Handicap is that in the Asian you can bet on quarters instead of just in halves.

Handicap	Team Results	Bet result	Handicap	Team Results	Bet result
0	Win	Win	0	Win	Win
	Draw	Refund		Draw	Refund
	Lose	Lose		Lose	Lose
	Win	Win		Win	Win

Handicap	Team Results	Bet result	Handicap	Team Results	Bet result
-0.25	Draw	Lose Half	+0.25	Draw	Win Half
	Lose	Lose		Lose	Lose
-0.50	Win	Win	+0.50	Win	Win
	Draw	Lose		Draw	Win
	Lose	Lose		Lose	Lose
-0.75	Win By 2+	Win	+0.75	Win	Win
	Win By 1	Win Half		Draw	Win
	Draw	Lose		Lose By 1	Lose Half
	Lose	Lose		Lose By 2+	Lose
-1.00	Win By 2+	Win	+1.00	Win	Win
	Win By 1	Refund		Draw	Win
	Draw	Lose		Lose By 1	Refund
	Lose	Lose		Lose By 2+	Lose
-1.25	Win By 2+	Win	+1.25	Win	Win
	Win By 1	Lose Half		Draw	Win
	Draw	Lose		Lose By 1	Win Half
	Lose	Lose		Lose By 2+	Lose
-1.50	Win By 2+	Win	+1.50	Win	Win
	Win By 1	Lose		Draw	Win
	Draw	Lose		Lose By 1	Win
	Lose	Lose		Lose By 2+	Lose
-1.75	Win By 3+	Win	+1.75	Win	Win
	Win By 2	Win Half		Draw	Win
	Win By 1	Lose		Lose By 1	Win
	Draw	Lose		Lose By 2+	Lose Half
	Lose	Lose		Lose By 3+	Lose
-2.00	Win By 3+	Win	+2.00	Win	Win
	Win By 2	Refund		Draw	Win
	Win By 1	Lose		Lose By 1	Win
	Draw	Lose		Lose By 2+	Refund
	Lose	Lose		Lose By 3+	Lose

Sports betting

This is the activity of predicting sports results and placing a wager on the outcome. There are different types of bets: fixed odds betting, live betting, pool betting (definitions follow).

Fixed odds

When bettors wager against odds. There are many distinct forms of fixed odds betting such as:

- Money line betting: this is a straight up bet where the player needs to predict the outright winner.
- Spread betting: a type of betting or wagering on the outcome of an event where the payout is based on the accuracy of the bet, rather than a fixed win or loss outcome.
- Parlay bets: a parlay involves multiple bets that reward successful bettors with a greater payout. A parlay comprises at least two bets but can have more.

Live betting (or in-play betting)

When bettors can place wagers while the event is in progress. This increases drastically the number of markets that are offered to the players in the sportsbook.

Pool betting

When bettors pay a fixed price into a pool. The pool is then evenly divided between those that have wagered the correct outcome. There are no odds involved.

L.6.1 Selecting the offer

Objective: To ensure the integrity of a betting offer.

L.6.1.1 - Betting framework

The framework in which the organization offers sports, esports and horse race 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.

Implementation guidance

Sports betting is a complex activity where the risks are high, especially if operators are not cautious about the betting frameworks. On top of this, local regulations and applicable laws are significantly distinct between the countries. This implies a need for strong operations controls.

The method of making bets in sports betting should be straightforward and understandable. Information should be made available so that the player is clearly informed of the details of the bet prior to making the bet. All selections in a bet should be displayed to the client. Sports betting offerings should help to prevent extended, continuous, and impulsive play.

1. The client should be informed whether his/her bet has been accepted or not.

2. Where the client has placed a bet and the odds, payouts, or prices of the bet change prior to the bet being confirmed by the operator, the client should have the option of confirming or withdrawing the bet (with the bet refund).

3. Where operators offer a client an option of automatic acceptance of changes in bets, the client should be able to manually opt out of this function at any time.

4. The client should be informed of the period in which bets can be made on an event or series of events and that bets cannot be placed after the close of the betting period.

5. Sports betting games should not mislead clients about the odds, payouts, or any element of a bet.

6. The client should be informed of the data source(s) that will determine the outcome of the bet.

The following is a list of minimum controls that should be present:

- A well-defined and accurate description of every betting type for which controls can be applied: some countries do not allow sports betting on any events so as to prevent sports corruption.
- Not all the bet types are authorized in every country: parlay bets, single bets, live betting.
- Well-defined and accurate description of specificities of each sport: for example, soccer rules are not the same for all the competitions. This needs to be communicated to the clients.
- Well-defined and accurate definition of each specific term related to betting offer: the operators do not always apply the same rules for the same bets. This needs to be communicated to the clients.
- Well-defined and accurate description of financial limits and gambling restrictions (i.e., restrictions on type of bet, possible bet combinations, amount of gain) the betting offer is usually wide. The operators have multiple ways to manage the offer. This needs to be clearly explained to the clients.
- Well-defined and accurate methods of computing of gain: odds may be displayed in different ways (American, fractional, decimal). Depending on the display, outcomes may be calculated distinctly. This needs to be explained to the clients.
- Well-defined and accurate terms of gain payments: the most important thing is to clarify the rules of resettlements that the operator will apply. Rules for cancellation of bets should be formally documented and tested. For example, when an event is suspended or cancelled or sometimes when the operator makes an obvious mistake.
- Well-defined description of the source of feeds: the operators may rely on providers for the source of feeds. The integrity of the source of feed must be dealt with carefully. The integration must be assessed.
- Sports betting rules must be publicly published. This is usually required by the regulator but even if this is not the case, the operator should clearly explain its practices to the clients.

- Local specificities of regulations: as mentioned above, the regulations may differ depending on the jurisdiction. For example, some countries require geolocation for the players. This needs to be assessed thoroughly.

Examples of audit evidence

- A documented list of controls clearly specified.
- An organizational framework for sports betting (traders, IT operators, risk managers, audit teams).
- Settlement procedures.
- Financial control procedures.
- List of incidents related to the offer selection.
- Risk analysis on the offer selection.
- Test plan of all the sports betting rules of play.

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

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 respect of integrity, responsible gaming, and ensuring transparency.

Implementation guidance

Events selection and odds compiling

Fixed odds in sports betting may change prior to and during an event. Changes in odds should be updated and made available to clients who have placed a bet on the event.

- The process of events selection and odds compilation should be properly logged and audited periodically.
- Events offered should be selected based on the best available judgment that the events are fair.
- Authorized levels for the margin of each bet type should be documented in the internal controls.
- Odds offered should reflect the best knowledge for the probability of the outcome of each event, adjusted for the operator's profit margin (over-round). Odds should be based on judgment of facts and not be based on opportunity or rumors.

Determination of betting results

Betting outcomes should be determined in accordance with the governing sports betting regulation and prevailing payouts as they are described to the client. The sports betting settlement process

should be conducted fairly, honestly and in accordance with the terms of the bet placed by the client.

Sports bets should be accepted, processed, and settled in accordance with the terms of the bet placed by the client, including any applicable betting rules.

The results of bets on sporting events should be provided to clients making bets on the events and be made accessible to the public. The results should include information that affects or affected the outcome of all bets for the event. Any change of results should be made available. For clients using their betting accounts, account balances will be updated as the results of bets are confirmed. For clients making bets not using accounts, clients will be entitled to payment for winning bets once results of the event are confirmed.

Sports betting operators should have controls in place to review the accuracy and timeliness of sports and events results data.

Qualifying betting results

Before publicly announcing results and declaring winners, there should be a policy for the confirmation of results based on qualified and approved sources of data, unless automated by an external and certified sports data feed.

- If an external feed is in use, there should be procedures in place for cases where access to the external feed is unavailable.
- There should also be a procedure in place to handle changes in results (e.g., due to statistics/line corrections).
- A backup record of all results and their changes should be kept and identified as a critical asset.
- Results' entry should include the entry of all information which may affect the outcome of all types of bets offered for that event.
- It should be possible for a player to obtain the results of their bets on any decided sports event once the results have been confirmed.
- Any change of results (e.g., due to statistics/line corrections) should be made available.

The operator determines if a bet is a winning bet based on the official sports event results. The scores and results for a game become the official sports event results when the operator enters the results in the sport betting system.

The internal controls should delineate how resettlement was done to correct errors such as:

- operator errors
- the sport's governing body changes a call on a particular play
- or final scores
- or a malfunction

which may cause winnings to be incorrectly credited to the player's account.

Reliability on external stakeholders

The reliability on external stakeholders involved in these activities should be qualified. Commitments on the reliability of their activities should be included in contracts to protect the organization against the financial and legal risks in case of incidents impacting third parties.

Nowadays, most of the activities for odds selections are automated by IT platforms. The integrity of these operations should be assessed technically. Organizations should ensure:

- Time accuracy of the transactions and events (timestamping, time sync).
- Integrity monitoring of critical IT components of the sports betting platform as well as logical access control.
- A thorough wager record management: everything should be logged.
- Geolocation by design should be possible to restrict the offer to a territory when required by regulation.

To ensure that the operations remain secure, two of the most important processes are the change management process and the security incident management process. Depending on the robustness of those processes, the risks of integrity will be correctly mitigated.

The change management process should be tested and assessed. Frequent weaknesses include:

- Clear notification to any third party that would be impacted.
- Clear notification to any third party that would be impacted.
- Risk and impact analysis of the changes.
- Categorization of the changes.
- Change validation.

The Security incident management process should be tested and assessed. Frequently weaknesses are:

- Crisis management and escalation procedures.
- Notifications to third parties.
- Classification of security incidents.

Examples of audit evidence

- A software architecture document that details the integrity measures of the platform.
- Access reviews of the platform.
- Reports on the critical components monitoring.

- Event logs on the sports betting platform.
- Change logs and change reports.
- Security incidents reports.

L.6.2.2 - Live betting

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 court siding prevention mechanisms including but not limited to a delay in live pictures.

Implementation guidance

Live betting events offered require automation in processing and efficiency and effectiveness in supervising and managing the lifecycle of such betting.

Live betting management is the same as for any other betting, only it is done quicker, and has a different workflow from pre-live. The betting platform has to allow traders to have an oversight of all betting offers within a game through an interface (live betting panel), which allows all of the lifecycle controls in a streamlined way - all of the game at their fingertips. Traders using this live betting panel will be keeping their eyes on the live game and/or live data coming from the game, and at market reference points outside of their application, as well as their live betting panel. Ideally at least three or four different screens are required to observe and make split-second decisions.

Context

An operator’s live betting platform should enable a live betting panel where traders are allowed to manage live betting offers and the betting itself through its lifecycle, from creation or opening to settlement.

Effective usage of the panel considering live betting relies on:

Integrated data services for automated creation of events and also:

- Majority of live betting markets
- Suggested odds for such markets.
- Reference sports data feed providers pricing
- Event 'ticks' and betting control messages (e.g. 'free kick taken' or 'suspend betting').
- Results.

Derivatives engine for live betting which:

- Derives odds based on 'base odds' and then derivation parameters.

- Recalculating odds with lapsed time and significant events (i.e., touchdowns, goals).
- Automates tradability statuses based on 'ticks' and betting control messages.
- Creates 'chain' markets (e.g., 'next something' – next scorer).
- Results and auto-settles markets.

Effective integration with the betting risk module to retrieve open positions in real time.

Manual entry of ticks and base prices when feed data is not available.

Live betting offering

The assumption is that the totality of the live betting offer will be comprised of the following elements:

- Using sports data provider fees: for a selected range of events and markets - everything is automated. This is for most of the offer where differentiation is not important.
- Manual live betting for a small number of selected events which are deemed important in at least one of the operating domains and are not adequately covered by data services. In this case the events and/or part of the results may come from the data service, but live betting is manual.

The controls should include:

- Live betting systems to ensure non-repudiation of bets.
- Commitment of supplier on integrity of betting data (rating) should be ensured prior to developing a live bet offering.
- Packages of betting data should contain a signature enabling the possibility to verify the integrity of data received (e.g., using hash functions).
- Authenticity of emitter and integrity of communication flows of betting data should be ensured (i.e., using secured protocols).
- Monitoring of live betting should be implemented to detect an unusual number of bets (considering time of the day), massive simultaneous connections, unusual number of wins, and all kinds of events which could be considered as suspicious given their unusuality.
- Monitoring of live betting should align with the local regulatory requirements.
- Conditions of settlement should be strictly defined according to local regulations and readable by all players. Player acceptance of these conditions should be required by the organization before allowing access to live betting.
- Operators should have procedures to allow players to complain.
- Operators should have a means to ensure the integrity of the results. Cryptography may be used to ensure the integrity of the logs (chaining and timestamping mechanisms are a good way to prevent unauthorized modification of the transactions).

- Where there is a derivative engine for live betting, additional controls should be in place to secure the offer.

Examples of audit evidence

- Architecture documents that demonstrate the integrity of communications between platform components.
- Monitoring procedures and/or alerts reports.
- Player's complaint procedures.
- Test cases about the integrity of the transactions in transit and at rest.

L.6.2.3 - Safeguarding payout levels

The organization shall establish a set of measures to ensure authorized payout levels are not exceeded.

Implementation guidance

Some regulations require the operators to guarantee the return to players rate (or at least to monitor it). Additionally, the operator must deal with its financial risks. Therefore, operators should define thresholds for restricting payout to acceptable limits and have indicators in place to be able to detect when the total payout exceeds these limits (the total amount of payout related to one account, the return to player rate for an event, the potential amount of payout related to one bet, etc.).

Examples of audit evidence

- List of controls in place to monitor payouts.
- Reports on the payouts.

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

Procedures shall be established to monitor all changes to odds and/or blocking throughout a sports, esports and horse race 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.

Implementation guidance

The organization should control its sports betting activities around four areas:

1. Financial control.

2. Event control.

3. Player control.

4. Internal control.

Financial controls

Financial risk monitoring, RTP rate, volume of wagers, i.e.

Event controls

Game event monitoring (bet types, odds, results promulgation). Subscribing to third party services such as the United Loteries for Integrity in Sports something to take into consideration to ensure the integrity of the sports events.

Sports betting operators should have risk management measures in place to mitigate the integrity risk associated with potential sport crimes linked to a sport event/betting:

- Operators should establish controls to identify unusual and/or suspicious betting activity and report such activity to an independent sports integrity monitoring body such as ULIS.
- Operators should ensure their sports integrity monitoring body shares information with other sports integrity monitoring stakeholders and promptly disseminate alerts/reports of unusual activity to all public and private stakeholders involved.
- All sports betting operators should review such alerts/reports and notify their sports integrity monitoring body of whether they have experienced similar activity.
- If a sports integrity monitoring body such as United Loteries for Integrity in Sports finds that previously reported unusual betting activity rises to the level of suspicious activity, they should immediately notify all other integrity stakeholders including law enforcement agencies, sport governing bodies and gaming authorities.
- All integrity monitoring providers receiving such an alert/report should share it with their member sports betting operators.
- Sports integrity monitoring bodies should, at a minimum, notify and promptly provide the following:
  - All alerts/reports of unusual betting activity,
  - If the activity was determined to be suspicious, and
  - The actions taken by the sports integrity monitoring body.

Independent sports integrity bodies should notify the relevant law enforcement agencies, sport governing bodies and gaming authorities upon detecting or becoming aware of any abnormal

betting activity or patterns that may indicate a concern about the integrity of a sports event(s) or any other conduct with the potential to corrupt the betting outcome of a sports event for purposes of financial gain, including but not limited to match fixing.

An operator receiving a report of suspicious activity may suspend or cancel the sports betting offer on events related to the alert/report. As a result, the operator must ensure that it has reserved itself the authority to suspend betting and to void all bets. The operator's decision to suspend or cancel sports and betting on events related to the alert/report must be reasonable and made in good faith.

Player controls

Player account activities monitoring (personal data modifications, financial moves).

Internal controls

Operators' activities monitoring, ITSM processes (change, incident, delivery), trading activities monitoring, training of the operators and traders for collusion and fraud mechanisms should be regularly performed.

Employees involved in performing control activities should be trained and have knowledge of the organization's control environment, the regulatory risks that the controls are designed to mitigate, and the regulatory objectives reflected in the certified betting regulatory framework of the jurisdiction.

Each operator should maintain an organizational structure that meets, at a minimum, the following criteria aimed at preserving the integrity of the betting and gaming operations:

- A system of personnel and chain of command allowing for the adjudication of responsibilities for actions and omissions.
- The segregation of incompatible functions so that no employees are in a position to both commit an error or perpetrate a fraud and, at the same time, conceal the error or fraud in the normal course of their duties.
- Primary and secondary supervisory positions which permit the authorization or the supervision of necessary transactions at all relevant times.
- Areas of responsibility which are not too extensive so as to be impractical for one person to monitor.

There should be a separation of duties to ensure that no group has overall control without oversight. The operator should set very clear work responsibilities to minimize mistakes, limit liabilities, and increase the amount of separation between related duties.

An internal organization structure should be in place, such as:

- Operators should have an internal audit department, either in a separate department within the betting and gaming operations, or using a corporate internal audit commission, or delegating said function to third parties.
- The internal audit department should maintain its independence through an organizational chain of accountability external to the management of the gaming operation contest.
- The internal audit department must consist of at least two internal auditors independent of the areas subject to audit (auditors internal to the operation, officers of the Commission, or an outside accredited organization may perform this function).
- The internal audit department should be responsible for auditing the compliance with these regulations, and technical standards or operational controls as adopted by these regulations, as well as to the laws and regulations provided by the gaming regulatory body and the prevailing internal controls.
- The internal audit department should carry out the following minimum functions:
  - Examine and evaluate the adequacy of internal controls.
  - Ensure that internal controls are complied with through observation and examination of accounting documentation.
  - Inform the operator of those instances in which internal controls are not observed.
  - Inform of any fundamental failure of the internal control system.
  - Recommend improvements to the internal control system, if necessary.
- The method by which the operator fulfills its requirements with respect to the internal audit department should be described in the operator's written table of organization.
- The internal audit department should be supervised by a key employee who holds an occupational license endorsed with the position of accounting officer.
- The employee of that function will report directly to the chief financial officer or compliance officer, the property's general manager, an off-property corporation executive, or an independent committee audit, as established by the operator.

Those controls should be monitored and trigger alarms, which must be followed, and investigated if needed to establish their basis.

Example of anti-fraud controls

- Follow-up recording of foreign credit cards.
- Identification of credit card used on more than one account.
- Identification of higher payments.
- Follow-up International Bank Account Number recording, and identification of players who record the highest numbers of International Bank Account Number.
- Identification of important amounts of cash-out or payments.

Examples of audit evidence

- List of controls in place for each areas.
- Reports on monitoring activities.

L.7 Interactive Video Lottery Terminals (VLT)

L.7.1 Video Lottery Terminals (VLT)

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

L.7.1.1 - VLT terminals

VLT terminals shall be monitored concerning security and prize payout percentage.

Implementation guidance

The monitoring of VLT terminals should be done according to the existing surveillance and incident procedure to ensure the correct prize payout to customers.

This control should be regularly audited or monitored.

Typically, automatic IT controls exist that warn the lottery if the prize payout is not according to game rules or decisions made by the lottery.

Examples of audit evidence

- Prize payout reports.
- Incident reports.
- Audit reports.

L.7.1.2 - VLT games

The game-rules and overall prize-payout percentage shall be available to the customer.

Implementation guidance

Customers playing VLT should have easy access to information about the VLT games, the gaming rules, and the prize payout structure.

Examples of audit evidence

- Prize payout information on the terminal.
- Prize payout information on wall posters.
- Prize payout information is given on the lottery's website.

L.7.1.3 - VLT game certificate

Dedicated games for VLT shall be tested and a certificate, to provide evidence of integrity and prize-payout, has to be maintained/issued.

Implementation guidance

VLT games should be properly security tested to ensure they are in compliance with gaming rules before putting them into production.

The security test of each VLT game should be documented with a game certificate.

Examples of audit evidence

- Game certificates issued by the lottery service provider or other trusted party.
- Game certificate register.
- Statements given by the lottery service provider.
- Security test report.

L.7.1.4 - VLT system architecture

The organization shall maintain a description of the overall VLT system architecture, including security measures, to ensure the integrity of the VLT game, secure storage and processing of data.

Implementation guidance

VLT system operation is often implemented differently among different lotteries.

To ensure that vulnerabilities of the VLT system are identified, and that proper security measures are in place, an architecture description can be used to identify and ensure the security and integrity measures implemented to control the VLT system.

Examples of audit evidence

- VLT system architecture figure.
- Process figure showing possible “single point of failure” or security weakness.
- List of implemented security and integrity controls

L.8 Random Number Generation

L.8.1 Randomness in electronic draws and chance-based digital games

Objective: To ensure the integrity and fairness of random number generators and drawing algorithms by physical and logical protection. L.8 covers electronic draw-based games and any chance-based digital games.

L.8.1.1 - Physical and logical protection of the technical system

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.

Implementation guidance

Physical aspects:

The identification of their physical location/hosting: data center, server room, dedicated technical room.

The identification of security measures: camera/CCTV, physical access control system, motion detectors, guards, and fire extinction system.

The management of physical access to the location of the RNG and drawing algorithms.

Logical aspects:

Technical documentation/evidence should be provided to highlight the following aspects:

Architecture:

- A secure architecture for the hosting of both components (i.e., RNG and drawing algorithm) in a multi-layer architecture.

Network:

- Network partitioning according to the following principles:
  - Different network areas should be defined according to the levels of sensitivity of these components.
  - The implementation of filtering and monitoring equipment to guarantee secure communication exchanges between both components.
  - A filtering policy to prevent any non-authorized access or modification.

System:

- The hardening of operating system should be defined.
- The connection policy should be defined: from the console where the RNG is hosted, from a remote connection, with a segregation of duties (role and connection profiles).
- The time source should be defined and there should be certainty as to the time source used.

The above should be fully auditable to align with best practice.

Examples of audit evidence

- Technical documentation of the electronic drawing system including the random generation components.
- Configuration audits reports on the implementation of the drawing system including the random generation components.

L.8.1.2 - Secured transmissions

Measures shall be taken in order to ensure integrity and authenticity of the data transmitted between the RNG (entropy source) and the drawing algorithm.

Implementation guidance

When both components are hosted on separated machines/appliances, technical documentation/evidence should be provided to highlight:

Network aspect:

- Identification of network protocol(s) used between both components to ensure confidentiality of information.
- Unique (or range) IP addresses used and dedicated for both components in these network protocols.
- Protocols and controls used to ensure integrity of the components.

System aspect:

- Authentication principle based on mutual authentication.
- System hardening and auditing.

Examples of audit evidence

- Technical architecture highlights the measures to ensure integrity and authenticity do the communications.
- Controls defined for supervision and monitoring of integrity and authenticity.

L.8.1.3 - Electronic draw randomness and integrity verification

Before deployment, tests and verifications shall be performed by independent parties in order to verify that the electronic drawing system is random.

The organization shall document its policy related to after-deployment tests and verifications in order to verify that the random number generator and drawing algorithm is performing as specified.

Implementation guidance

A drawing system may be sliced into different core functionalities. The RNG source (either True Random Number Generator or Pseudo Random Number Generator) and the draw routines. Depending on the use case, the drawing system may be integrated in the game engine.

The core objectives of the controls shall be:

- To ensure good quality randomness of the RNG source and correct usage of this source by the application.
- To ensure that the software is using the RNG source correctly and securely.
- If the application is using a remote RNG (hardware not installed in the server running the application), checks must be performed to ensure that the application is obtaining the random numbers from the correct source and to ensure the integrity of these transactions.
- If the application requests random numbers at a higher throughput than the RNG can provide, it should have a fail-safe behaviour.
- If the application receives an error from the RNG when it requests random numbers, it should have fail-safe behaviour.
- To ensure that the transformation of raw random numbers does not introduce bias.
- To check the randomness of draws generated by each routine and check that results are compliant with the routine specification (Diehard tests, NIST SP 800-22 tests, Chi squared tests).

In the case of a PRNG the core objectives of the controls shall be:

- To ensure that the software is using a good quality Pseudo RNG algorithm and that it uses this RNG source correctly and securely.
- To ensure that the PRNG type and usage are correct.
- To ensure that the PRNG seeding, reseeding, and buffer management are correct.
- If it is necessary to guarantee the traceability of draws in the gaming engine, the following checks must be done in order to ensure that it is possible to validate the draws using an audit system (knowing a seed, it possible to reproduce the draws in order to check that there was no cheating for these draws).
- If the application encounters an error when using the PRNG, it should have fail-safe behaviour. Blocking / non-blocking configuration

And this may include:

- To ensure non-repudiation of game actions and bets.
- To ensure that the game engine configuration is compliant with the engine specifications and that the audit trail is configured properly.
- A mass data test should be performed on each game to check each of the prize level odds.

In any case, these tests should:

- Be realized before new implementation of a game in production.
- Be realized by an external independent body (such as the international gaming test labs or any national test lab authorized by the lottery).
- A report on the test results should be prepared.
- The scope of the audit and the audit baseline should be clearly defined.

The above-mentioned processes should be defined in a policy.

Examples of audit evidence

- A policy on after-deployment tests and verifications.
- The reports of the tests.
- A document that describes the drawing system with full transparency (no security by obscurity).

L.8.1.4 - Segregation of duties

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

Implementation guidance

There should not be a single person (or team) who can impact the integrity of an electronic draw without oversight.

It is desirable to have separate people performing no more than one of the following types of duties: designing/implementing/maintaining the draw system, monitoring the system, or performing draws. Note that this best practice is broader than the requirement, which does not extend to design and implementation.

Examples of audit evidence

- A list of the roles and their roles in the main activities of the electronic draw.
- A list of identified critical roles where collusion could occur.
- Segregation of duties rules.

L.9 Online games

L.9.1 Randomness in electronic draws and chance-based digital games

Objective: To ensure secure operation of games

Online game: Refers to all gaming related activity delivered through mobile application or web-based online platforms, but not including retail transactions.

L.9.1.1 - Online game rules

The online game-rules and overall prize-payout percentage shall be available to the customer.

Implementation guidance

Customers playing online games should have easy access to information about the online games, the gaming rules, and the prize payout structure.

Examples of audit evidence

- Online game rules, prize payout percentage stated for each game on lottery's website or mobile app.
- Online game monitoring of payout percentage.
- Online game monitoring of prizes that exceeds gaming rules.

L.9.1.2 - Online games certificate

Dedicated online games shall be tested and evidence shall be provided to assure integrity and correct prize-payout throughout the whole lifecycle of the game.

Implementation guidance

Online games should be properly security tested to ensure they are compliant with gaming rules before putting them into production. The security test of each online game should be documented with a game certificate. The lottery should have procedures to make sure that the online game certificate is controlled and formally approved.

Examples of audit evidence

- Online game certificates issued by the third party supplier or other trusted party.
- Online game certificate register.
- Security test report issued by the service provider or other security testing entity.
- Lottery procedures related to approving online game certificates.

L.9.1.3 - Online games exit

Procedures shall be established to handle when online games are taken out of production, hence take in consideration how to handle Jackpots not won.

Implementation guidance

Online games usually follow a 4 steps life cycle process (develop, test, production, and termination). Some online games remain in production for a long time and some also have Jackpots. Lotteries that offer online games with Jackpots should have procedures in place to control when the online game is terminated, and the Jackpot is not won. Information about how non-won Jackpots will be handled should also be reflected in the game rules given to the customer.

Examples of audit evidence

- Lottery procedure on handling online game Jackpots is handled.
- Online games status register.
- Information to customers about Jackpots and how they are handled.

L.9.1.4 - Discrepancies of online game results

Procedures shall be established to handle discrepancies between what is presented on customer's digital devices, and what is logged in the gaming system.

Implementation guidance

Online games are mostly offered to customers as "game-as-a-service" and are often a managed service by a third party (ref. G.5.3). Customers also use different devices to play online games. Customers using their devices do not always update lottery apps to the newest approved version. Third party online game suppliers need to take this into consideration as possible discrepancies that could lead to incidents.

Lottery suppliers should have in place security procedures to control possible discrepancies, misconfiguration to online games, including information to the customer on how this will be handled.

Lotteries should have procedures to undertake investigations and secure sufficient evidence in case of a customer dispute. This can be done using replay functionality, logging, or audit file investigations.

Examples of audit evidence:

- Online game rules giving information to customers about how discrepancies will be handled.
- Replay functionality on online games.
- Online game transactions logging, available to lotteries.
- Security test report issued by the service provider or other security testing entity.

L.9.1.5 - Security of games with pre-determined winners

For games that have pre-determined winners, procedures shall be established, based on a risk analysis, to ensure that no one can take advantage of the game mechanisms.

Implementation guidance

Most online games are pre-determined. Online games should be sufficiently security tested to ensure the game's integrity. Some online games can be played as multi-player games and have elements of skills or can be stopped before it automatically is ended.

Irregularity, misconfiguration, fraud attempts or disputes between the lottery and the customer could lead to integrity or security issues.

Lotteries should identify possible risks related to possible misconfiguration, fraud or other irregularity to games that are considered as multi-player or skill based. Relevant procedures to control the risks identified should be implemented.

Examples of audit evidence

- Risks assessment related to online games that are considered as multi-player or skill based.
- Procedures to monitor and detect irregularities and possible fraud situations.

L.10 Game design and approval

L.10.1 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.10.1.1 – Documented game rules

Game rules shall be documented and accessible by players.

Implementation guidance

The organization should ensure that players always have the possibility to easily consult the game rules.

Depending on the local laws or regulations, game system frontends should show a banner that warns players of risks, displays the main rules of the game, or links explicitly to the rules of the game.

Example of audit evidence

- A publicly accessible document that lists the rules of games in their entirety.

L.10.1.2 – Game approval and modification

An approval procedure shall be defined to validate that every new game and relevant modifications on the digital gaming systems are controlled. Final game design shall be formally approved through a process involving the security function.

Implementation guidance

New games or game modifications should be subject to a security risk analysis.

Corrective measures should be identified by the Security Function and implemented for identified flaws or weaknesses, according to their level of severity.

The remaining risks should be formally accepted by management in accordance with the Security Function.

A game should not be offered to the public until the Security Function has formally approved it.

Examples of audit evidence

- Risk assessments and associated action plans.
- Formal approval by the Security Function for the production launch of new products or new versions of existing products.
- The minutes of management's formal approval of the residual risks.

L.10.1.3 – Gaming Supplier selection

The security function shall be involved in the approval process.

Implementation guidance

Lotteries that procure games from a gaming supplier (def. 3.2) or procure gaming services (def. 3.2) should as part of the procurement process have procedures detailing the security requirements in Annex C (S controls).

Those procedures should involve the security function, so no controls are forgotten or removed.

Gaming suppliers can become a WLA certified entity and ensure that their security and integrity requirements are sufficiently implemented.

The security function should take into account that if the gaming supplier is WLA certified:

- The certificate is valid.
- The certificate covers the gaming services that the lottery procures.
- The Statement of Applicability includes all relevant S controls.

If the gaming supplier is not WLA certified the lottery should ensure that the gaming supplier can demonstrate compliance with the S controls.

Examples of audit evidence

- Security function approval process procedure.
- Gaming supplier security status register.
- Audit report on gaming supplier.

Annex C (S Controls) Controls for the development of gaming systems and the provision of gaming services

Applicability: The S controls apply to the development of gaming systems and the provision of gaming services, whether that be a gaming supplier or the gaming operator's own in-house developers. In the case that a gaming operator or gaming supplier acquires a gaming system or services from a third party, it is the gaming operator’s or gaming supplier’s responsibility to assure compliance to these S controls from the third party.

S.1 Gaming systems security assurance

S.1.1 Gaming system application secure development

Objective: To ensure gaming systems are secure by design.

S.1.1.1 - Application development security policy

There shall be a policy on application security across the software development lifecycle.

Implementation guidance

The policy should be available upon request. It should be in accordance with OWASP® requirements (or similar) for what is determined safe programming practices. The policy should be provided as part of an on-boarding practice for developers.

Over and above the implementation guidance in ISO/IEC 27002 for a secure development policy best practice to meet this control would include specific considerations on ensuring gaming systems are designed to operate with the highest levels of integrity.

Examples of areas that might be included are:

- Where code re-use should be encouraged and where it should be discouraged, and how any code re-use will be managed through the lifecycle, considering the extent to which dependency checking and similar should be integrated to minimize vulnerabilities in the gaming system code.
- Consideration should be given to preventing secrets from being hardcoded.

- Policy on to what extent potential vulnerabilities identified (e.g., through static code analysis) require fixing prior to the code being checked into the code repository, or prior to a production release.
- Controls required to be in place to ensure the integrity of sensitive areas of the code base (i.e., that could impact game integrity).

Examples of audit evidence

- Application development security policy.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.1.2 - Security testing

The organization shall perform security testing of their products and/or services.

The organization should adjust the tests based on the nature of the change, considering the impact and level of risk associated with it.

The organization shall provide to the operator:

- An inventory of the tests performed during the software development lifecycle. This inventory must cover all principal risks.
- A summary of the output along with the release notes for their product for the first release and any subsequent significant release into a production environment.

Implementation guidance

There should be a clearly defined chapter for security testing including a list of tests performed. It should specify what is tested, how regularly, and the values that need to be protected and tested. The testing procedures should be adapted to the context and the size of the entity.

The type of testing conducted should be commensurate with the risk posed by the changes being introduced into the system.

The risk assessment should follow these steps:

- Identify critical assets.
- Identify threats.
- Estimate probabilities and impacts.
- Evaluate the risks.
- Recommend mitigation measures.
- Reassess risks.

Moreover, special attention should be given to ensuring that the test cases adequately cover the identified risks, addressing the most critical scenarios and potential vulnerabilities related to the change. Each change to an IT system can present different potential risks, and the gaming technology supplier should assess these risks appropriately. As an example, in a major upgrade that involves significant changes in code and functionality, it is essential to perform extensive security testing to ensure that the new functionality does not create vulnerabilities. However, when the change only affects the back end of a solution, for example, with no direct impact on functionality or end-user interactions, it may be justified not to perform extensive penetration testing. In this case, it would be better to focus on other types of security testing, such as static code analysis or integration testing to ensure system stability.

Testing should follow a recognized methodology such as, but not limited to, OSSTMM or OWASP®. Testing should be only conducted with sufficient experience and competency and those testing the change should be independent (but can reside in the same organization) of those who have designed or developed the change.

Here are some examples of relevant tests that could be included in the policy (the list is not exhaustive):

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Software Composition Analysis (SCA)
- Penetration Tests
- Secret detection
- Vulnerability scanning
- Network scanning
- Code review

For each change, the inventory of the tests performed during the software development lifecycle shall be documented, and the outputs shall serve to feed a logic of action plans for security development.

Examples of audit evidence

- Summary of the security testing output provided by the supplier to the operator.
- Output from risk assessment
- Summary of security testing output as part of release notes.

S.1.1.3 - Representativeness of the security tests

The security tests conducted by the gaming technology supplier shall reflect how the system will be deployed in a production environment by the operator.

Implementation guidance

Testing should be on infrastructure and application representative of the production environment. The gaming operator might risk assessing the different components of the gaming system and determine that they are comfortable relying on any testing already being undertaken by the gaming operator/supplier on some of the components of the gaming system. The supplier of the gaming system should not assume a gaming operator will conduct testing themselves and the default position of the supplier of the gaming system is that they should plan to conduct testing themselves to provide assurance over the security of the products and services they are supplying.

It is important that the security tests conform to the production environment for several reasons:

- Accuracy of results: Security test results are only relevant if they reflect the reality of the production environment.
- Minimize risk: Security testing can be disruptive to the production environment. Ensuring that tests are consistent with the production environment minimizes the risk of disruption or damage.
- Better understanding of vulnerabilities: By using data and configurations that reflect the production environment, security testing can provide a better understanding of specific vulnerabilities that affect the production environment.

In order for security testing to reflect reality, it is important to:

- Use realistic data and configurations: Security testing should be performed using data and configurations that reflect the production environment. For example, system test data, SQL test data, performance test data.
- Use appropriate configuration: Tools used for testing purposes should be configured in the same way as they will be used in the production environment
- Plan tests to minimize disruption: Security testing can be disruptive to the production environment, so it is important to plan tests to minimize disruption. For example, tests can be scheduled to run during off-peak hours.

When testing on production environment cannot be avoided, great care should be taken.

Examples of audit evidence

- Test and production environment configuration files.

S.1.1.4 - Secure coding practices

Secure coding practices shall be defined and required for developers to follow and there shall be measures to audit the effectiveness and compliance of those practices.

Implementation guidance

The secure coding practices should complement principles of good software architecture and be documented such that, if asked for, they are available upon request. The coding practices should be

able to be easily applied by developers to the languages that are actively in use by the organization.

Examples of audit evidence

- Documented secure coding practices.
- Procedures to audit the effectiveness and compliance of secure coding practices.
- WLA-SCS:2024certificate for any gaming system supplier(s).

S.1.1.5 - Secure coding training and awareness

There shall be a training and awareness program on secure coding practices for all developers that write code for gaming systems.

Implementation guidance

There should be a system that shows the current “awareness-level” of a given set of developers, such that a given level of compliance can be shown. Best practice would be to test levels of security awareness on recruitment and on a minimum of an annual basis thereafter. Furthermore, if a developer fails the test, and subsequent intervention does not enable them to pass a repeat test, then their access to work on the gaming system code should be revoked.

Examples of audit evidence

- Training and awareness program for developers.
- Metrics showing, for example, how many developers at the supplier who are working on systems used by the operator have passed secure coding training and awareness training in the last year.
- WLA-SCS:2024 certificate for any gaming system supplier(s).

S.1.2 Integrity measures related to the development of gaming system hardware, software, and firmware

Objective: To ensure integrity of gaming technologies.

S.1.2.1 - Release process integrity checks

There shall be assurance over the integrity of the 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.

Implementation guidance

Best practice would be to have documented procedures for checking the integrity of code using, for example, hash values or code signing to ensure the same code that was written is the same code that is testing and is the same code that will end up in the production environment.

Examples of audit evidence

- A procedure documenting the checks conducted.

S.1.2.2 - Security logging

There shall be adequate security logging provided from the developed software / firmware, that can be integrated by a security team into their security toolsets to ensure the integrity of the software/ firmware. There shall be a document that details how to interpret and understand the security logging.

Implementation guidance

A vendor should be able to provide logging of who has done what, and when, in a format that can easily integrate with SIEM-systems to be correlated against other log sources. Where event codes or similar are used, they should be documented so that they are easily understandable. There should be sufficient coverage in the logs of any change that could impact on gaming system security.

For clarity, while the control refers to software and firmware, access to critical data and configuration files is also within the scope of this control.

In this instance “security team” is the team responsible for monitoring the gaming system when it is operational in the production environment, whichever organization they reside in.

Examples of audit evidence

- Documentation for the interpretation of logs.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.2.3 - File integrity

Critical files in the product shall be identified and documented in order for the gaming operator to verify the integrity of the production environment.

Implementation guidance

The supplier should consider the files that could impact game integrity for the components they are responsible for, or for the components they are dependent on, from an integrity perspective lower down the technology stack.

Those files might be included in the product as a result of compiled code they have developed or third-party code they have re-used, as a result of middleware, operating system files of any hypervisor or containers in use, databases, data files or configuration files, etc. (note this is not an exhaustive list).

Where possible a file “manifest” should be given with a given release that states which files are what, and what their unique hash is. This is to verify that files remain unmodified. This can enable a

gaming operator to introduce audit capabilities to detect changes in files made by unauthorized users.

It is recognized that the above guidance does not work for dynamically generated files. In these cases, this control requirement might not be possible to be met by the supplier.

Examples of audit evidence

- Documentation on critical files provided by the supplier to the operator.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.2.4 - Hardware integrity

There shall be measures put in place to allow for the identification of unauthorized attempts to add or modify the gaming system hardware that could impact the integrity of the gaming system. In this

context hardware includes as a minimum, but is not limited to, video lottery terminals, gaming 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.

Implementation guidance

The party developing and maintaining the gaming system should perform the risk assessment and make it available to the lottery operator upon request.

Tamper-evident seals, or even better, tamper-evident alarms that can be remotely monitored would be best practice here.

Examples of audit evidence

- Documentation detailing the measures put in place by the supplier for the identification of threats to hardware integrity.
- Procedure detailing how the above measures are to be checked and verified.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.2.5 - Vulnerability and patch management

There shall be 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 gaming operator’s vulnerability and patch management policy and taking into account any commercial considerations.

Implementation guidance

The supplier has a responsibility under this control to ensure there is a process and tooling in place to identify new vulnerabilities, and a mechanism to patch them in a timely manner, that the operator can make use of if they choose to do so.

Not in this control is the lottery operator's responsibility to make a decision on whether to patch and to carry out the patching in a timely manner.

Examples of audit evidence

- Processes in place for monitoring and vulnerability and patch management.
- Tools used for monitoring and vulnerability / patch and dependency management.
- Software development tickets where the above has been implemented.
- WLA-SCS:2024 certificate for gaming system suppliers.

S.1.2.6 - Responsible disclosure

A gaming 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.

Implementation guidance

There should be a policy and associated process for dealing with responsible disclosures. This should identify where reports should be made and how rapidly they will be assessed and acted on (if necessary). Effort investigating and responding to reports of responsible disclosures should not incur any cost on the part of the organization making the report.

Examples of audit evidence

- Responsible disclosure policy and processes of the supplier(s).
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.3 Integrity measures related to printing of physical instant tickets

Objective: To ensure integrity of gaming technologies.

S.1.3.1 Physical instant game requirements

Objective: To align supplier specification to gaming requirements.

S.1.3.1.1 - Instant game requirements

The manufacturer shall formally validate requirements with the gaming operator and translate those requirements into specifications; any change in the specifications shall follow both supplier's and

gaming operator's change management process.

Implementation guidance

In order to guarantee that, gaming operator's requirements are met, the printer/supplier could apply the following measures:

- Establish exhaustive specifications that match the lottery operator requirements.
- Ensure that the gaming operator formally validates specifications.
- Should any changes occur to the specifications, ensure that the gaming operator formally validates them.

Examples of audit evidence

- Any formal document demonstrating the validation of specification by the lottery operator.
- Documented change request process.
- WLA-SCS:2024 certificate for gaming system supplier(s).

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

The randomization process used for the generation of instant game data is subject to the application of WLA-SCS L.8 Random number generation controls and the requirements agreed between the operator and supplier.

Implementation guidance

The printer/supplier should implement all controls from chapter L.8 of WLA-SCS. For more details, refer to the Code of Practice for L.8 For the avoidance of doubt, game generation systems for physical instant tickets are considered Gaming Systems as defined in this standard.

Examples of audit evidence

- Any document confirming that the supplier has included WLA-SCS:2024 L.8 controls in its statement of applicability.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.3.2.2 - Game data validation

The ticket manufacturer shall ensure that an independent team validates logical game data against gaming operator requirements. Reports with results shall be made available to the gaming operator.

Implementation guidance

The supplier can ensure game data integrity through the following measures:

- The supplier should mandate an independent team (internal or external) to audit the programed prize structure and to make sure that it matches the lottery requirements.
- Should the prize structure balancing be flexible in the specifications, the supplier will formally communicate the final prize structure to the operator.

Examples of audit evidence

- Any audit report established by an independent auditor.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.3.2.3 - Data confidentiality

The ticket manufacturer 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.

Implementation guidance

Game data leaks can be prevented through the following measures:

- The supplier should classify and consider validation data as a high value asset in relation to confidentiality.
- There should be specific logical and physical access controls to guarantee confidentiality; the principle of least privilege should be strictly implemented.
- Personnel with access to game data should be made aware of its level of confidentiality and of the measures in place to protect it.

Examples of audit evidence

- Any information security certificate issued by a third party; should an ISO/IEC 27001 certificate be produced; the auditor should check that the related Statement of Applicability includes A.9 controls.
- Observation of physical access control.
- Any proof related to access authorization.
- Any document showing reconciliation between effective access and related authorizations.
- Any protocol confirming that authorized employees have received awareness training related to data confidentiality.
- Observation of incident list.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.3.3 Printing

Objective: To ensure integrity features in the printing process.

S.1.3.3.1 - Validation before printing

The ticket manufacturer shall formally validate the final visuals and texts with the gaming operator before printing tickets.

Implementation guidance

The supplier can ensure that lottery operator's requirements are met by requesting the gaming operator to formally validate the digital contract proof with the final visuals and texts.

Examples of audit evidence

- Any formal document proving the operator validation of final visuals and texts.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.3.3.2 - Integrity checks

The ticket manufacturer shall perform integrity audits on tickets on a regular basis.

Implementation guidance

The supplier can guarantee tickets' opacity and conformity to requirement through the following measures:

- The supplier should take printed ticket samples on a regular basis (depending on the production size) in order to perform integrity audits that include quality and security checks.
- Security checks should include opacity, mechanical, and chemical tests.
- Quality checks aim to verify that tickets meet the lottery operator's requirements and that the game can be played.
- Any change to the production, like for example to the paper or ink, should be followed by an integrity audit.

Production samples should be taken on a very regular basis in order to identify a specific ticket range in an incident context.

Examples of audit evidence

- Observation of production samples collected during printing. Observation that samples quantities are sufficient to identify a specific ticket range in the context of an incident.
- Any security quality check protocol.
- Any document (audit report, test protocol, authorization protocol) showing that change management has been implemented in the printing environment (ink, paper).
- WLA-SCS:2024 certificate for gaming system supplier(s).

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

Provisions shall be made for each ticket delivered to have a unique reference number.

Implementation guidance

The supplier can guarantee that every ticket has a unique reference number through the following measures:

- The supplier should formally establish in the requirements the printing method it plans to use.
- Should some tickets be printed more than once, resulting in having multiple tickets with the same number, the supplier should ensure that the irrelevant tickets are scrapped. The traceability of those tickets is essential to prove the state of every ticket and to make sure there is no incident.

Examples of audit evidence

- Any document showing that the printing methodology has been notified to the operator.
- A list of the tickets that have been printed more than once, with the same reference number.
- Any protocol confirming that those tickets have been scrapped.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.3.4.2 - Prize structure conformity

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.

Implementation guidance

The supplier can guarantee that the final prize structure of delivered tickets conforms to the requirements through the following measures:

- The supplier should have game data audited against the operator’s requirements, in order to ensure that the number of tickets is in line with the required prize structure. This verification can take the form of an audit performed by an independent team (internal or external).
- An audit report should be formally established and should be sent or kept available for the operator.

Examples of audit evidence

- Audit reports.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.3.4.3 - Scrapped tickets

There shall be a documented procedure to ensure that undelivered printed tickets are securely destroyed.

Implementation guidance

The supplier can guarantee that no ruled-out ticket can be put on the market through the following measures:

- The supplier should be able to prove the scrapping of any book of tickets through traceability. That means the supplier should establish a formal listing of scrapped book numbers.
- In order to prevent the tickets from being stolen, physical access to tickets to be scrapped should be scrapped. In addition, the use of a temporary secured bin with a one-way opening is recommended.
- Scrapping has to be monitored and formally protocoled.
- Scrapping can include security shredding or burning the tickets

Examples of audit evidence

- List of printed books (a list of the books delivered, and a list of the books scraped).
- Book scrapping protocol.
- Observation of supplier incident list to check eventual books lost. Any books lost must be investigated.
- WLA-SCS:2024 certificate for gaming system supplier(s).

S.1.3.4.4 - Shipping security

The supplier shall ensure that ticket delivery between the supplier and the gaming operator is secured.

Implementation guidance

The supplier can ensure that shipping is secured and that any theft during shipping is detected through the following measures:

- The supplier should use, whenever possible, a non-shared container that is locked with a seal identified with a unique number. The seal number has to be sent to the operator before shipping. The operator should match the ship number at delivery. This measure is especially recommended for operators that do not manage tickets activation through their information system.

Examples of audit evidence

- Any document related to transport protection.
- Any communication between the printer and the client operator mentioning the seal number.
- Any document issued by the client operator that acknowledges the delivery.

- WLA-SCS:2024 certificate for gaming system supplier(s).

Annex D (M Controls) Controls for multijurisdictional games

Applicability: M controls apply to operators that participate in games run by the Multi-State Lottery Association (MUSL).

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

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.

Implementation guidance

The MUSL Minimum Game Security Standards is a confidential document describing the requirements for validation and audit of claims. This document must be provided only to persons with responsibility for design, execution, or audit of the claim validation process.

As part of joining or continuing to participate in MUSL games, lotteries will be provided with this document and must demonstrate how the lottery's processes implement the requirements in the document.

Examples of audit evidence

- Validation procedure documents.
- Completed validation packets/folders with documents showing validation were completed.
- In-person walkthrough with auditor of the validation process.
- Observation of physical devices used for validation.

M.1.1.2 - Redundancy of transaction data

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.

Implementation guidance

The gaming system must consist of systems in at least two locations that are not likely to be subject to
the same disaster. Transactions must be recorded to both systems before and at the same time as the
transaction becomes official, i.e., when the ticket is printed.

- **Examples of audit evidence**
- The address or location of each computer gaming system, distance measurement (e.g., Google Maps) showing they are sufficiently separated.
- Disaster recovery plan / risk analysis showing how the two locations are not likely to be subject to the same disaster.
- Documentation showing the process of recording a transaction on each system to show that a record will exist in at least two distinct datacenter locations.
- Review technical documentation that shows that the terminal waits for acknowledgement from at least two production Computer Gaming System before printing a ticket.

M.1.1.3 - Acknowledgement of transaction

Each location shall receive and acknowledge transaction board data prior to a ticket being allowed to print.

Implementation guidance

See the implementation guidance of the control **M.1.1.2**

Examples of audit evidence

See the examples of audit evidence of the control **M.1.1.2.**

M.1.1.4 - Backup of play data

Play data must be backed up daily and stored offline and offsite.

Implementation guidance

In addition to L.5.1.2, M1.1.4 requires play data to be backed up daily offline and off-site. Off-site is generally well understood and essentially means not subject to the same disaster (**see M.1.1.2**). Additionally, data must be backed up offline daily. This helps reduce loss of data from accidental deletion, corruption, malicious encryption, i.e. the offline data does not need to be taken off-site if the
off-site requirement is met through other means.

Examples of audit evidence

- Documentation/example of when backups are collected, where they are stored, and how they are stored for both the Internal Control System & Computer Gaming System.
- Description/documentation showing the process for capturing data offline at least daily.
- If off-site backup is not continuous, confirmation that the data is captured off-site at least daily. The offline and off-site backups do not have to be a single copy or device, storing data on geographically separated online systems and daily tape/unplugged media backups at only one is acceptable.

M.1.1.5 - Integrity of transactions before and after a draw

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.

Implementation guidance

The ICS must automatically verify that its copy of the transactions has not changed from before to after
the draw. It must do this by hashing the transactions before the draw, saving the hash, and then hashing
the transactions after the draw and ensuring the resultant hash matches the original.

MUSL approved hash algorithms are generally determined by the list of hash algorithms approved for
use by the US National Institute of Standards and Technology (NIST). A hash algorithm is a one-way function that is infeasible to reverse. For example, given input A, hash function H, and output B=H(A), it is easy to verify B given A, but infeasible to determine A given B since there is no inverse hash algorithm or function.

Examples of audit evidence

- Documentation showing that a hash of all transaction data is created on the Internal ControlSystem before each draw. Show that the Internal Control System produces a hash of the same data immediately following the draw.

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

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.

Implementation guidance

The NASPL API Specification is available to lotteries participating in MUSL games. Section 7, Security, list requirements for transaction flow and security.

Examples of audit evidence

- Detailed technical documentation of the data flow process between the retailer points of sale and the Computer Gaming System, including all systems where the data is not encrypted, and where encrypted data is combined in a central point (e.g., a retailer back-office system).

M.1.2.2 - Lottery terminals not intended to produce live tickets

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.

Implementation guidance

The most common method is to use "void" paper and install locks on the printers so the paper cannot be changed other than by lottery security. Other methods are the removal of a pin from the print head, or a physical font change (this may be outdated as there are likely no lotteries using impact printers anymore).

Examples of audit evidence

- Observe all terminals in areas that are accessible to personnel with access to the gaming system or internal control system. Those terminals must be modified so that any tickets printed are clearly not valid tickets.

M.1.3 Quick picks

Objective: To ensure that quick picks are selected randomly.

M.1.3.1 - Randomness of quick picks

Software used to generate random numbers for quick picks shall comply with WLA-SCS control **L.8.1.3** “Electronic draw randomness and integrity verification”.

Implementation guidance

See the implementation guidance of control **L.8.1.3**

Examples of audit evidence

- Independent party's documented certification that the electronic drawing system performs as expected for every game that it is required to make quick pick selections for.

- Provide documentation on the organization's policy for verifying that the random number generator is performing as specified after deployment.
- See also the examples of audit evidence of control **L.8.1.3.**

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.

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.

Implementation guidance

Ensure that only the lottery and vendor staff have access to the systems on their own respective networks. This would include firewall, ICS/CGS OS, ICS/CGS server access, and any additional systems that may provide access to the ICS, CGS or transactional data. Review user access controls for these systems.

Examples of audit evidence

- Exports of user accounts from the live systems, including OS, application, network hardware, AD/LDAP.
- Interview with managers/staff inquiring about job roles of selected users.
- Review of system diagrams showing which systems are part of which area.

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.

The lottery or its authorized designee shall process winning numbers using the same personnel and the same ICS systems used for processing sales transactions.

Implementation guidance

There should not be a shift change during the normal draw processing time for a game.

Examples of audit evidence

- Observe shift calendars and query staff/management about normal shift times.

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

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.

Implementation guidance

All systems must use a network or host-based Intrusion Detection System (IDS) or Intrusion Prevention System (IPS).

Examples of audit evidence

- Provide screenshots or other documentation that confirms an intrusion detection or prevention system is in place on both ICS and CGS networks and shows that they remain up to date.
- Show proof of notification from these systems to local administrators.

Code of Practice for the WLA-SCS:2024 (CoP:2024)

Version 1.3 Publication: December 2024 Latest revision: December 2024

This document is the property of the World Lottery Association (WLA) and contains confidential information. It may not be transferred from the custody or control of WLA except as authorized in writing by an officer of the WLA. Neither this document nor the information it contains may be used, transferred, reproduced, published, or disclosed, in whole or in part, either directly or indirectly, except as expressly authorized by an officer of the WLA, pursuant to written agreement.

PLATINUM Contributors

Gold Contributors