WORLD LOTTERY ASSOCIATION

Code of Practice for the WLA-SCS:2020

CoP:2020

Version 1.0
Publication: August 2021
Latest revision: August 2021

Contents

Foreword

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

The WLA Security 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 Control Standard (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.

This is the first edition of the Code of Practice for the WLA-SCS:2020 (CoP:2020).

Introduction

The CoP:2020 was previously introduced in the portmanteau of WLA-SCS documentation in 2021. It contains implementation guidelines and examples of audit evidence for the WLA-SCS:2020 controls.

This document has been written by the WLA SRMC, incorporating relevant comments and feedback received by WLA-SCS auditors and WLA members, received either via email or through the WLA Wiki[1]. The CoP:2020 remained publicly available on the WLA Wiki from February 16th, 2021, until April 16th, 2021.

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

With the CoP:2020 the WLA aims to support the understanding and the application of WLA-SCS:2020 controls at a global level.

[1] https://wiki.world-lotteries.org

Scope

The CoP:2020 is designed to support:

- WLA members that are organizing their Information Security Management Systems in preparation for a WLA-SCS:2020 assessment.
- WLA-affiliated auditors conducting WLA-SCS:2020 assessments of WLA members.

Some of implementation guidelines shown within this document extend the scope of the corresponding controls of the WLA-SCS:2020. In this case, following the expanded interpretation of the control provided by the implementation guidance should be considered as best practice only.

Normative references

The following documents are normatively referenced throughout the CoP:2020 and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 27001 Information Technology – Security techniques – Information Security Management Systems – Requirements.
- ISO/IEC 27017 Information Technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- WLA-SCS:2020.
- Guide to Certification for the WLA-SCS.

Terms and definitions

For the purposes of this document, the terms and definitions given in WLA-SCS:2020 apply.

Annex A (G Controls) for all organizations

Applicability: G controls apply to lottery and gaming operators, as well as to 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

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, lotteries 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 role of the responsible committee or group to take ownership of security risks, but rather its role 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.

The security forum should report regularly and directly to the board committee responsible for enterprise risk management. To this end, there should be permanent and full representation of the security forum on the relevant board committee.

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/IEV 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.

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 show 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 lottery is organized.

It is also the role 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 no lower than executive level management and shall be independent of the technology 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 lottery actively consider 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, in order 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 reporting line should be moved or a dotted reporting line to another executive should be put in place.

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 be sufficiently empowered and shall have access to all necessary resources to enable 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 business 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

G.2.1.1 – Code of conduct

A code of conduct shall be issued to all personnel when initially employed.

All personnel 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 based on the definition of personnel included in the WLA-SCS:2020, the code of conduct is not solely applicable to employees. It also applies to contractors or other third parties who work for the lottery operator or lottery technology supplier and, by virtue of their role or access, have the potential to impact the confidentiality, availability, or integrity of the lottery.

While it is fine to have a single code of conduct, it is also acceptable for an organization to issue different versions of the code of conduct: one for those on the payroll of the organization and one for third parties (e.g., contractors) working with the organization.

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 personnel 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. For personnel who are not directly employed by the organization (e.g., contractors), where disciplinary action is not relevant, alternative, and appropriate procedures should be referenced.

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 personnel are required to declare conflicts of interest on employment as and when they occur. Specific examples of conflict of interest shall be cited within the code.

Implementation guidance

Personnel 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, personnel should inform the organization. An example of a conflict of interest would be when an employee of a lottery with a technology function also has a role in, or owns shares in, the company of the developer of the independent control system (ICS).

Example of audit evidence

- The code of conduct section that requires declarations 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 obligate all personnel 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 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 of 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 lottery 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 lottery as well as any prize claims, against those who are prohibited to play, 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 people 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 lottery 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 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 of integrity. This might be anything from ensuring the integrity of a certain area of code, or a configuration file on the server, on through to 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. In the context of a lottery technology supplier, this control shall relate to critical areas of code that could impact the integrity of a game such as, but not limited to, handling the input-to-output from random number generation used for determining the outcome of games.

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 employees or roles where collusion could occur.
- Segregation of the duty rules.

G.2.2 Staff protection

G.2.2.1 - Policy on staff protection

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

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 lottery 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 employee.
- Process for checking on staff who are conducting lone working.

G.3 Physical and environmental security

G.3.1 Secure areas

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.

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

Examples of audit evidence

- Automatic or manual log showing access to datacenter.
- 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

G.4.1.1 - User access functions

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

Implementation guidance

Permissions 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.

Example of audit evidence

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

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.
- Trigged alarms or incidents.

G.5 Information systems maintenance

G.5.1 Cryptographic controls

G.5.1.1 - Cryptographic controls for the confidentiality of data at rest on portable systems and on lottery terminals.

Cryptography to protect the confidentiality of information shall be applied for sensitive information on portable computer systems (end user devices e.g. laptops, removable media e.g. USB devices, and similar) and to protect the integrity of sensitive information held at rest on lottery terminals.

Implementation guidance

This control relates to the confidentiality and integrity of information at rest on a device. 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. Lotteries 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, as long as 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 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.

Examples of audit evidence

- Group policy on a Windows system that enforces Bitlocker encryption on laptops and removable media.
- Test to show 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 different 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

G.5.2.1 - Test methodology policy and data

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 will the transformation 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 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 be only conducted by those with sufficient experience and competency. 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 as part of this control (G.5.2.2).

Examples of audit evidence

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

G.5.3 Cloud security

G.5.3.1 - Cloud security

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

Implementation guidance

ISO/IEC 27017 provides cloud-specific implementation guidance to a range of ISO/IEC 27001 controls and adds several new cloud-specific controls to the lotteries' ISMS.

Lotteries that host their gaming systems in a cloud environment should choose a cloud provider that can demonstrate compliance to ISO/IEC 27017. Note that the control refers to compliance and not certification, thus it does not require a certification process.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models (for more details on the definition of cloud computing see NIST SP 800-145).

An operator or supplier should have adequate documentation as part of its ISMS to demonstrate compliance to the cloud service customer aspect of ISO/IEC 27017. There are some questionnaires on cloud security available online that could be used to verify if a system is compliant with ISO/IEC 27017. It is worth mentioning that the vast majority of the controls contained in the ISO/IEC 27017 are built on already existing ISO/IEC 27001controls. In the ISMS that organizations have in place, auditors might expect to see references on how those controls are applied in a cloud environment.

If a cloud provider cannot show compliance with ISO/IEC 27017, an acceptable alternative could be to show compliance with the Cloud Security Alliance® Cloud Controls Matrix (CSA CCM), as the CSA CCM maps to, and exceeds the requirements of, ISO/IEC 27017. While this covers the cloud provider, the lottery or lottery supplier should also ensure that the controls of ISO/IEC 27017, that they are responsible for as a consumer of cloud services, are still met. At this time, compliance with other standards is not accepted as way of meeting this control requirement, although the WLA SRMC will keep the position under review.

Lottery suppliers should note that, while code repositories are specifically mentioned, if the suppliers also host gaming systems (e.g., game data generation or reconstruction systems used for instants), and those systems are hosted in the cloud, then they are also subject to this control.

It is not a pre-requisite for WLA-SCS auditors to have detailed training in, or knowledge of, ISO/IEC 27017, given that it follows the same principles as ISO/IEC 27001. Although auditors should understand the concepts behind the public cloud sufficiently to assess compliance with this control requirement.

Examples of audit evidence

- Statement of compliance from the cloud service provider's auditor.
- ISMS of the lottery with the ISO/IEC 27017 requirements included.

G.6 System availability and business continuity

G.6.1 Availability of services and business continuity

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 lottery 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. By articulating availability requirements an organization can settle the cost vs risk tradeoff with regard to architecting resilience and redundancy into their systems.

Examples of audit evidence

- List of system showing availability requirements.
- Monitoring reports of present availability.

Implementation guidance

G.6.1.2 - Business continuity

The organization shall prepare a documented business continuity plan that covers, at minimum, the continued operation of lottery games and continued stakeholder confidence in the integrity of lottery operations. The organization shall furthermore plan, perform, and evaluate business continuity exercises in regular intervals to prepare the organization for crisis situations, covering the elements included in the business continuity plan.

Organizations should have a resilience plan to ensure that services can be provided in a crisis. 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 of time, 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.

WLA-SCS auditors are not required to know the ISO/IEC 22301 standard in order to assess this control, in the same way that ISO/IEC 27001 lead auditors are not required to know the ISO/IEC 22301 standard to assess the business continuity management controls in that standard.

Examples of audit evidence

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

Annex B (L Controls) for lottery operators

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

L.1 Physical instant tickets

L.1.1 Instant game operations

L.1.1.1 - Printer/Supplier selection

There shall be a formal approval process which involves the security function.

Implementation guidance

To mitigate game integrity risks, the process leading to the formal approval of a printer/supplier should be documented. The process should involve the security function. Best practice shows that the security function's involvement should begin in the early stages of the approval process. Here are some examples of how this involvement could be realized:

- Definition of security requirements in call for tender.
- Evaluation of the conformity / scoring of tenders in relation to security requirements.
- Analysis of the certifications provided by the printers/suppliers; verification of their relevance (field, scope, control exclusion), and their validity. Verification of the printer/supplier certification against controls of section S.1.3 of WLA-SCS:2020.

Examples of audit evidence

- Presence of a documented approval process for the selection of printer/supplier that involves the security function.
- Security requirements, coming from the security function, in the request for proposals or contract.
- Any evidence (meeting minutes, evaluation report, etc.) demonstrating that the security function was involved during the evaluation process of the printer/supplier.

L.1.1.2 - Integrity requirements and testing

The organization shall implement a documented procedure that covers the entire game lifecycle, from design to destruction, by specifying the integrity requirements for each instant game. The integrity requirements shall include at least, but not be limited to, the following: final visuals and text, prize structure, protection of validation/winner files, quality controls, auditable inventory to account for the distribution, location of packs, and adequate testing of the requirements before the game is accepted.

Implementation guidance

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, etc.); 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 of quality controls should include, but not be limited to the following areas:
    - Programming
- Compliance with game mechanics.
- Compliance with prize structure.
- Compliance with specifications for the distribution of tickets in the books (Guaranteed Low End Prize Structure – GLEPS), if applicable.
    - Printing
- Non-predictability of a ticket's winning status based on visible information.
- Ticket opacity tests: Using various techniques to determine whether a ticket is a winning ticket without scratching it or without visibly altering it.
- Tests
    - Internal quality and security tests (by the printer).
    - Lottery operator quality and security tests.
    - Independent laboratory tests.
- 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.
    - Investigate book loss and report 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.1.1.3 - 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.1.1.2. 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 privilege 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 implemented.
- 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, that describes security requirements for game data that is transferred to the lottery operator.
- Evidence of the controls applied by the lottery.

L.1.1.4 - 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 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 the 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:

- Obtain assurance that the printer/supplier is adequately protecting game data containing the list of tickets with the ticket winning status, while it is on their premises.
- Ensure that ticket validation data sent by the printer/supplier is encrypted; apply segregation of duties to protect the encryption key.
- Treat the location of a book of tickets as confidential. Inform personnel, that has access to this information, about the risks related to the protection of this information (i.e., social engineering).
- Establish a formal procedure for ticket reconstruction requests sent to printers and monitor its use. The list of reconstruction requests could be sent by the printer/supplier directly to an independent entity inside the lottery for review (it could be the security function)
- To eliminate doubt, reconstruction request portals and reconstruction systems, given their critical significance, should fall under the definition of gaming systems in regard to this standard.

Examples of audit evidence

- 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

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 principles 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 (depending on applicable regulations), etc.
- 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, etc.

Example 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 draw process – before, during, and after –should be formalized. The operational procedures should be defined for each range of game.

Each range of game, includes:

- The different steps for each range of games. The description of each step should answer the questions: 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 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, GSM.

Examples of audit evidence

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

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

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 the section L.2.1., a control check list should be specified for each main function in the draw process, by range of game.

Example 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 the 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 responsible individual for each action, the material required, the deadline for each action, and the control actions should all be identified.
- The draw step: The responsible individual 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 responsible individual 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 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 game.
- Depending on the game (i.e., EUML), 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 done.; 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 (seen in 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 these 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 phone.
- 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 participants.
- The material necessary for the draw and for the announced results.

Examples of audit evidence

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

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 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 draws.

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, etc.).

Examples of audit evidence

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

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).
- The description of the draw equipment and how it works. This includes the description and use of the draw sphere, the description, and the use of the balls for each draw.
- Controls should be set to check the operational procedures.

Examples of audit evidence

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

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 manage 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, medias, etc.).
- 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 actions plan should be specified with the owner of each action.

Examples of audit evidence

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

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 of 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

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 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 detail of each maintenance level should be specified.
- The traceability of each maintenance intervention should be defined.

A global planning of the 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.

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

Example of audit evidence

- Technical Procedure.

L.2.4 Electronic lottery draws and instants

L.2.4.1 - 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: datacenter, 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:
  - A network partitioning according to the following principles:
    - Different network areas should be defined according to 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 OS 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.
- Configuration audits reports on the implementation of the drawing system.

L.2.4.2 - Secured transmissions

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

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

L.2.4.3 - Electronic draw randomness and integrity verification

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

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

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 behavior.
- If the application receives an error from the RNG when it requests random numbers, it should have a fail-safe behavior.
- 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 a fail-safe behavior. Blocking / Non-blocking configuration (/dev/random, /dev/urandom)

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 of the tests 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.2.4.4 - Segregation of duties

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

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

L.3 Retailer security

L.3.1 Retailer operations

L.3.1.1 - Retailer security

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

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

L.3.2.1 - Transaction security

The data traffic between the gaming terminals and the central gaming system shall be protected and measures to ensure the integrity of the transactions shall be implemented. Where a retailer point of sale device is used instead of a dedicated lottery terminal, the data traffic from the lottery application on the point of sale device to the central gaming system must be protected and not be reliant on the security of the retailer point of sale device for the integrity of lottery 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, etc.) 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 the 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 in case 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 indicating 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 a point-of-sale equipment.

L.4 Prize payment

L.4.1 Validation and payout of 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 on through to their validation mechanism at the time the bettor claims a prize.

To generate the winning transactions, the systems in charge of the task would have to 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 controlled to verify that the ticket is correct.

The unique reference identifier 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 parallels 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 with 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

The correct implementation of this control is very important since there are several antecedents of employees who have tried to carry out a fraud by collecting unclaimed prizes.

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 will be 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 Unique Ticket Reference), 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 specification, 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 the 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 hits.

It is very important to specify the conditions for a ticket to be considered valid. Tickets with damaged or illegible barcodes or identifications 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; etc.
- A section or paragraph on payment procedures according to the amount of hits.
- A section or paragraph of the documents where the taxes or withholdings on the hits 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 employees 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 hit 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 hits. 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 hits collected near the expiration period. The selection of the sample and the periodicity of the control should be representative of the number of hits.

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.5 Digital sales channels and interactive services

L.5.1 Digital gaming systems

L.5.1.1 - Layered systems architecture

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

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. In particular, assets that are exposed on Internet shall be separated from other types of assets.
- A secure interconnection gateway (DMZ area) should be deployed in order to protect internal layers of the information system from Internet flows. This area should be considered as neutral and losable, as its hosted assets.
- 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 in order to detect inconsistencies or out-of-date parameters.
- Sensitive assets are not directly accessible from 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.

L.5.1.2 - Active and passive attacks

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

Implementation guidance

Prevention:

Risk assessments should be executed on every digital gaming system. Every new build phase and every evolution in run phase should be subject to a risk assessment as part of a process of change management, to evaluate their impact on the information system.

Action plans should be made and executed in order to reduce the criticality of risk that was identified in the risk assessments.

A continuous vulnerability watch should be established.

Policies of patching should be formalized that detail:

- The methods of the system components inventory.
- The information sources related to the publication of updates.
- The tools used in patch deployments and applications.
- The different steps and systems involved prior to production deployment.
- Obsolescence management.

A back-up strategy should be defined in policy and detailed by operational procedures (at least a back-up strategy and a recovery test).

A steering committee should be organized and should meet periodically in order to review indicators of detection and reaction efficiency (e.g., the number of detected malware, the number of vulnerabilities identified, the number of confirmed cyberattacks, response delay, etc.).

Detection and reaction should be periodically tested in a continuous improvement approach, and associated procedures updated when necessary.

Detection:

- The components of digital gaming systems are journalized according to requirements defined in risks assessments.
- Logs should be centralized in order to research suspicious events, archive logs, and avoid log erasing by attackers on compromised equipment.
- Real-time, updated, anti-malware protection should be deployed and managed using a centralized administration console.

Reaction:

- A process of incident response should be defined and documented with operational procedures.
- A process of crisis management should be defined and documented with operational procedures.
- Communication on security incidents and crises, both internal and external, should be defined in policy and documented with procedures.

Examples of audit evidence

- A patch management policy.
- A list of security measures / processes.

L.5.1.3 - Network segregation

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

Implementation guidance

Systems are designed following n-tiers models.

Databases and other sensitive assets should not be directly exposed on the Internet.

Filtering equipment should monitor flows between frontend and backend systems. Configuration is restricted to operational needs. Rejection is the norm, and authorization is the exception to the rule.

Filtering equipment should never be mutualized between frontend systems and backend systems. At least two physical devices shall be implemented.

Administrative resources should be deployed either:

- In a dedicated physical network or
- In a dedicated logical network, with utilization of IPsec VPN for protection administration flows. Logical segmentation and network filtering is recommended to restrict the exposure of the VPN concentrator to the administration workstations only.

Logical segmentation should be implemented between different sensitivity business activities.

Examples of audit evidence

- Technical Architecture documents.
- Network diagrams showing segmentation and filtering.

L.5.1.4 - Session information

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

Implementation guidance

A user session identifier should be generated with an RNG algorithm that has sufficient entropy.

User session identifier should be encrypted with state-of-the-art protocols when it is transmitted in order to prevent interception and modification.

Validity of sessions should be of finite duration.

Sessions should be linked to IP addresses and require reauthentication in case of change.

Examples of audit evidence

- User session identifier specifications.
- Audit reports on the user session identifier.

L.5.1.5 - Identify points of ingress and egress

All entry and exit points to open public network systems shall be identified, managed, monitored and controlled. The organization shall monitor all its digital gaming systems in order to prevent, detect, mitigate, and respond to cyberattacks.

Implementation guidance

A map of entry and exit points should be created and maintained.

Network infrastructure should be documented (e.g., network filtering policy, network diagram, flow matrices, equipment list).

Specific attention should be paid to the logging of activity on entry and exit points, as well as to the review of flow matrices on entry and exit points.

Prevention or/and detection systems should be deployed to monitor activities on entry and exit points

Examples of audit evidence

- A map of entry and exit points should be created and maintained.
- Network infrastructure should be documented (e.g., network filtering policy, network diagram, flow matrices, equipment list).
- External scan of the lottery's public IP range.

L.5.1.6 - Generation and storage of logs

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

Implementation guidance

A logging policy and associated procedures should specify the conditions for ensuring an audit trail:

- The generation of logs should include an adequate level of detail.
- The generation of logs should not retain authentication secrets nor personal information. Compliance with regulations and Information Systems Security Policy is essential.
- The generation of logs should include time stamping from synchronized time sources.
- Retention time should respect operational and regulatory requirements.
- Log storage should be secure in order to prevent loss or manipulation.

Examples of audit evidence

- Logging policy.
- Procedures for logging.

L.5.1.7 - Security testing

There shall be appropriate security testing on major system changes. Regular intrusion testing that attempts to identify and exploit vulnerabilities or other system weaknesses shall be performed at minimum on an annual basis

Implementation guidance

The security level should be proven during build and run phases of projects.

Build:

- Project management should include security by design in its approach. This includes security specifications that lead to particular implementations.
- Proper implementation of functional and security specifications should be assessed with specific automatic and/or manual controls (code audit, architecture audit, etc.).
- The reliability of solutions and products, and the impact that their integration has, should be assessed in a dedicated environment.
- The validation phase for risks assessment requirements should precede the production release/launch.
- Penetration testing and configuration audits should be performed prior to production release/launch of a new service or product.

Run:

- The addition of functionalities should be validated beforehand through risk assessments. Associated risks should be mitigated through palliative and/or compensatory measures.
- Major changes should be subjected to penetration testing and configuration audits.
- The impact of changes should be assessed in a test environment prior to production deployment.
- Continuous observation of vulnerabilities and vulnerability scans should be done in order to mitigate the risk of security breaches throughout the project life cycle.

Example of audit evidence

- Vulnerability scans.
- Penetration test reports.
- A security test strategy.
- Code audits or configuration audit reports.

L.5.1.8 - Responsible disclosure

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

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 lottery-branded, Internet-facing websites.

Example of audit evidence

- Responsible disclosure policy

L.5.2 Player account

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 are in agreement 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 perimeter of gaming offers.

Example of audit evidence

- Procedures for identification, authentication and authorization or 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 so as 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 or players.

L.5.3 Game design and approval

L.5.3.1 - Documented game procedures

Established rules shall cover design and development. In addition, game rules shall be 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 game in their entirety.

L.5.3.2 - Game approval and modification

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

Implementation guidance

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

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

The remaining risks should be formally accepted by the 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 of 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.5.4 Securing payment methods

L.5.4.1 - 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 lottery should consider what data is strictly needed for the transaction and only that data should be collected.

Example of audit evidence

- Data classification and identification defined in a data repository (baseline). Examples of audit evidence.

L.5.4.2 - 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 could refer to international standards, such as the PCI-DSS 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.5.4.3 - Payment service approval

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

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 (cf. PCI DSS certifications).

Examples of audit evidence

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

L.5.4.4 - Transactional records related to payments

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

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 in order 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 betting

L.6.1 Selecting the offer

L.6.1.1 - Betting framework

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

Implementation guidance

In accordance with local regulation and applicable law, the organizational framework should contain:

- A well-defined and accurate description of every type of bet and the sport upon which the bets can be applied.
- A well-defined and accurate description of the specifics of each sport.
- A well-defined and accurate definition of every specific term related to the betting offer.
- A well-defined and accurate description of the financial limits and gambling restrictions (i.e., restrictions on the type of bet, possible bet combinations, the amount of gain, etc.)
- A well-defined and accurate method for computing the gain.
- A well-defined and accurate term for gain payments
- The specifics of local regulations.

The organization should also document the technical platform supporting sports betting activities and should detail the procedures as to how this technical platform is managed and administered.

Examples of audit evidence

- An organizational framework for sports betting.
- A procedure to manage the technical platform for sports betting.

L.6.2 Events, odds, and result management

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

The organization should select its sport betting offer in accordance with local applicable laws and regulations.

The reliability on external stakeholders involved in these activities should be qualified, and 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.

For a definition of 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.

Example of audit evidence

- Procedures for selection of sport events, odds, and results management.

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

Implementation guidance

Live bet offering:

- Live betting systems should ensure the non-repudiation of bets.
- The commitment of the supplier on the integrity of betting data (rating) should be ensured prior to the development of a live-bet offering.
- Packages of betting data should contain a signature enabling the verification of the received data's integrity (e.g., using hash functions).
- The authenticity of the emitter and the integrity of the betting data communication flow should be ensured (i.e., using secured protocols).
- The monitoring of live betting should be implemented in order to detect an unusual number of bets (considering time of the day); massive, simultaneous connections; an unusual number of wins; and any events that could be considered unusual or suspicious.
- The monitoring of live betting should align with the local regulatory requirements.

Result handling:

- The availability of the systems responsible settlements should be ensured and/or the organization should be able to retrieve, after a delay, the data required for determining the win or loss of a bet.
- Contracts with third parties involved in the settlement process should include Service Level Agreements to guarantee their availability.
- The conditions of settlement should be strictly defined according to local laws and regulations and be made available to all players. Player acceptance of these conditions should be required by the organization before players can be allowed access to live betting.

Customer protection:

- The design of the live betting offering should comply with local laws and regulations regarding customer protection.
- The organization's frontends should contain a banner warning player of the gambling dangers.

Example of audit evidence

- Procedures for live bet offering, result handling, and customer protection.

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

The organization should define thresholds for restricting payouts to limits specified by local laws and regulations and the organization's own internal policies.

The organization should have indicators in place (e.g., the total amount of payout related to one account) and be able to detect if the total payout exceeds these limits.

Examples of audit evidence

- Internal policies and procedures.
- Supervision indicators or alerts.

L.6.3 Monitoring for fraud and 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 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 axes:

- Financial control: financial risk monitoring.
- Event control: game event monitoring (bet types, odds, declaration of results, etc.).
- Player control: player account activity monitoring (personal data modifications, financial moves, etc.).
- Internal control: player activity monitoring in terms of the organization and its collaborators.

These items should be detected, subject to alarm, followed up on, and investigated if need be.

Examples of anti-fraud controls:

- Follow-up of foreign credit card recordings.
- Identification of credit card use on more than one account.
- Identification of higher payments.
- Follow-up of IBAN recordings, and the identification of players who record the highest numbers of IBANs.
- Identification of significant amounts of cash-outs or payments.

Example of audit evidence

- Procedures for selection of sport events, odds, and results management.

L.7 Interactive Video Lottery Terminals (VLT)

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 report.

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 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 incidents

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

Implementation guidance

When an incident occurs, the customer might want to claim a prize payout or dispute on 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 equal cases are handled in the same way, the dispute process should describe how this is ensured.

Examples of audit evidence

- Written routines that describe the dispute or protest process.
- Examples of protest handling.

L.7.1.5 - VLT system architecture

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

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 integrity of the VLT system.

Examples of audit evidence

- VLT system architecture figure.
- Process figure showing possible “single point of failure” or security weakness.

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

Applicability: S Controls apply to suppliers and to lottery and gaming operators. When applicable, the S Controls are mandatory for suppliers and gaming operator claiming conformity to the WLA-SCS.

To be noted that during the assessment of operators, auditors will be confronted with one of the following situations:

a) The supplier of the certifying member is WLA-SCS:2020 certified. The WLA-SCS:2020 certificate of the supplier will suffice as evidence of compliance for all the applicable S controls.
b) The supplier of the certifying member is not WLA-SCS:2020 certified. The auditor should verify that all activities that require validation procedures and/or a documentation exchange between the operator and the supplier are assessed. The auditor shall ensure the operator can provide proof of integrity and security of gaming products and services provided by the supplier or an agreed risk treatment plan between the lottery and the supplier is in place.
c) The WLA member lottery maintains a proprietary gaming system, designed by its own in-house developers. In this case, all applicable controls of WLA-SCS:2020 Annex C shall be assessed.

S.1.1 Gaming system application security development

S.1.1.1 - Application development security policy

The lottery technology supplier shall have 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 of developers.

Over and above the implementation guidance in ISO/IEC 27002 for a secure development policy (ref 14.2.1), 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:2020 certificate for gaming system supplier(s).

S.1.1.2 - Static and dynamic code analysis

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

Implementation guidance

Static and dynamic code analysis tooling should be built into code pipelines and executed a minimum of once per release. Best practice would be to run the tools automatically and more frequently to provide a continuous feedback loop to developers, enabling them to address any issues found as part of the current development cycle and before changes are committed and submitted to testing en route to production.

What a “significant release” is will be the decision of the lottery operator.

Examples of audit evidence

- Software development tickets showing the results from code analysis tools have been considered.
- Output from code analysis tools.
- Summary of code analysis output as part of release notes.
- WLA-SCS:2020 certificate for gaming system supplier(s).

S.1.1.3 - Security testing

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

Implementation guidance

There should be a clearly defined policy for security testing that specifies what should be tested, how regularly, and the values that need to be protected and tested. This policy should require that both the scope and results of such tests are well documented and can be delivered upon request.

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 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.

Testing should be on infrastructure and application representative of the production environment.

The lottery operator might risk assess the different components of the gaming system and determine that they are comfortable relying on any testing already being undertaken by the lottery operator on some of the components of the gaming system. The supplier of the gaming system should not assume a lottery 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.

Examples of audit evidence

- Policy for security testing.
- Summary of the security testing output provided by the supplier to the operator.
- WLA-SCS:2020 certificate for gaming system supplier(s).

S.1.1.4 - Secure coding practices

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

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:2020 certificate for any gaming system supplier(s).

S.1.1.5 - Secure coding training and awareness

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

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 secure 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, working on systems used by the operator, have passed secure coding training and awareness training in the last year.
- WLA-SCS:2020 certificate for any gaming system supplier(s).

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

S.1.2.1 - Release process integrity checks

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

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

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

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 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:2020 certificate for gaming system supplier(s).

S.1.2.3 - File integrity

The lottery technology supplier shall identify and document critical files in their product in order for the lottery operator to verify the integrity of the production environment.

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 in order to verify that files remain unmodified. This can enable a lottery 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:2020 certificate for gaming system supplier(s).

S.1.2.4 - Hardware integrity

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

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:2020 certificate for gaming system supplier(s).

S.1.2.5 - Vulnerability and patch management

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

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:2020 certificate for gaming system suppliers.

S.1.2.6 - Responsible disclosure

The lottery technology supplier shall have a Responsible Disclosure Policy that is available to all those who have purchased their products or services, for the disclosure of security vulnerabilities in their gaming system products.

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:2020 certificate for gaming system supplier(s).

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

S.1.3.1.1 - Instant game requirements

The supplier shall formally validate requirements with the lottery and translate those requirements into specifications; any change in the specifications shall follow both supplier's and lottery's change management process.

Implementation guidance

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

- Establish exhaustive specifications that match the lottery operator requirements.
- Ensure that lottery operator formally validates specifications.
- Should any changes occur to the specifications, ensure that lottery 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:2020 certificate for gaming system supplier(s).

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.2.4 electronic lottery draws, and instants controls and the requirements agreed between the operator and supplier.

Implementation guidance

The printer/supplier should implement all controls from chapter L.2.4 of WLA-SCS. For more details, refer to the Code of Practice for L.2.4. 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:2020 L.2.4 "Electronic lottery draws and instants" controls in its statement of applicability.
- WLA-SCS:2020 certificate for gaming system supplier(s).

S.1.3.2.2 - Game data validation

The supplier shall ensure that an independent team validates logical game data against lottery requirements. Reports with results shall be made available to the lottery.

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:2020 certificate for gaming system supplier(s).

S.1.3.2.3 - Data confidentiality

The supplier shall ensure that access to validation data is restricted at all times, even after instant game delivery, in conformity with the principle of least privilege.

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 SOA 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:2020 certificate for gaming system supplier(s).

S.1.3.3.1 - Validation before printing

The supplier shall formally validate the final visuals and texts with the lottery before printing tickets.

Implementation guidance

The supplier can ensure that lottery operator's requirements are met by requesting the lottery 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:2020 certificate for gaming system supplier(s).

S.1.3.3.2 - Integrity checks

The supplier 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, as 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, etc.).
- WLA-SCS:2020 certificate for gaming system supplier(s).

S.1.3.4.1 - Unique ticket reference number

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

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 to having multiple tickets with the same number, the supplier should ensure that the irrelevant tickets are scrapped. Traceability of those tickets is essential to prove the estate 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 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:2020 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:2020 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 restricted. In addition, the use of a temporary secured bin with a one-way opening is recommended.
- Scrapping has to be monitored and formally protocolled.

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:2020 certificate for gaming system supplier(s).

S.1.3.4.4 - Shipping security

The supplier shall ensure ticket delivery between the supplier and the lottery 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:2020 certificate for gaming system supplier(s).

Annex D (M Controls) for multijurisdictional games

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

M.1.1 Security, integrity, and availability of transactions

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 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 was 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 or 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 no fewer than two distinct datacenter locations.
- Review technical documentation that shows that the terminal waits for acknowledgement from at least two production CGS 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, etc. 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 ICS and CGS.
- 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 the needed 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 ICS before each draw. Show that the ICS produces a hash of the same data immediately following the draw.

M.1.2 Security of retailer point of sale device

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 point of sale and the CGS, 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 persons 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

M.1.3.1 - Randomness of quick picks

Software used to generate random numbers for quick picks shall comply with WLA-SCS control L.2.4.3 “Electronic draw randomness and integrity verification”.

Implementation guidance

See the implementation guidance of the control L.2.4.3.

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 the control L.2.4.3.

M.1.4 Separation between ICS and CGS

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 staffs 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, etc.
- 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

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

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 IDS or 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:2020 (CoP:2020)

Version 1.0
Publication: August 2021
Latest revision: August 2021