INTERNATIONAL WORKSHOP AGREEMENT

IWA 17

First edition
2014-12-15

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

Informations et exigences d'intégrité et de sécurité relatives aux opérations pour la loterie et l'organisation de jeux

Reference number
IWA 17:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

International Workshop Agreement IWA 17 was approved at a workshop organized by the World Lottery Association (WLA), in association with the Association française de normalisation (AFNOR), and held in Zurich, Switzerland, in September 2014.

International Workshop Agreement IWA 17 is based on WLA-SCS:2012, *WLA Security Control Standard — Lottery and Gaming Security and Integrity Standard for Operations*.

Introduction

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

This International Workshop Agreement describes a security management process that is aligned both with internationally recognized standards and with a common security baseline for specific aspects relating to lottery and gaming organizers, which represents good practice. It comprises a comprehensive set of requirements, controls and standards for lottery and gaming organizers, including conformity with all requirements stated in ISO/IEC 27001 for information security management systems (ISMS).

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

The adoption of this International Workshop Agreement is a strategic decision for a lottery and gaming organizer. The design and implementation of the organization's Security and Integrity management systems are influenced by their specific needs, objectives, risks and security requirements, the processes employed and the size and structure of the organization. These factors and their supporting systems are expected to change over time and it is to be expected that a management system implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple Security and Integrity management system.

Compliance with this International Workshop Agreement can be used by interested internal and external parties to evaluate the security and integrity of a lottery and gaming organization.

This International Workshop Agreement is aligned with ISO/IEC 27001 and ISO 9001 to allow for consistent and integrated implementation and operation with related management system standards.

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

1 Scope

This International Workshop Agreement covers all types of lottery and gaming organizations, including commercial enterprises, government agencies and non-profit organizations. This International Workshop Agreement specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented security and integrity system within the context of the organization's overall risks. It specifies the requirements for the implementation of security and integrity controls applicable to the needs of individual organizations, so that the security and integrity management systems can be designed to ensure the selection of adequate and proportionate security and integrity controls that protect assets and give confidence to interested parties.

The requirements set out in this International Workshop Agreement are generic and are intended to be applicable to all organizations, regardless of type, size and nature.

NOTE 1 If an organization already has an operational business process management system (e.g. in relation with ISO 9001 or ISO 14001), in most cases it is advisable to satisfy the requirements of this International Workshop Agreement within the existing management system.

NOTE 2 Lottery and gaming organizers adopting this International Workshop Agreement are responsible for its correct application.

2 Normative references

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

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

3 Overview

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

Confidence in a lottery operation is key to retaining players and other stakeholders. Lottery and gaming organizers, therefore, need to develop and maintain a visible and documented security and integrity environment.

This International Workshop Agreement describes the requirements, control objectives and controls that are seen as best practice. A lottery and gaming organizer shall operate an information security management system that implements all requirements stated in ISO/IEC 27001, as well as the mandatory requirements and controls of this International Workshop Agreement.

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

In addition to general security and integrity management requirements contained in this International Workshop Agreement, Annexes A and B specify the minimum controls necessary for the effective management of security and integrity in a lottery and gaming organization.

4 General security and integrity management requirements

4.1 Information Security Management System (ISMS)

The organization shall operate an Information Security Management System (ISMS) that satisfies the requirements stated in ISO/IEC 27001.

4.2 Scope of the ISMS

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

4.3 Statement of applicability

The organization's ISMS statement of applicability shall explicitly include all controls in Annexes A and B. No control shall be excluded, but some of the controls in Annex B may be non-applicable. Claims of non-applicability shall be justified in detail.

Excluding any of the requirements specified in this clause (Clause 4), as well as any control in Annexes A and B, is not acceptable when an organization claims conformity to this International Workshop Agreement.

Any non-applicability of controls of Annex B found to be necessary needs to be formally justified and evidence needs to be provided that the non-applicability has been accepted by accountable people of the organization. Where any controls are non-applicable, claims of conformity to this International Workshop Agreement are not acceptable unless such exclusions do not affect the organization's ability and/or responsibility to provide security and integrity that meets the requirements as determined by a risk assessment and applicable statutory or regulatory requirements.

5 General security and integrity control objectives and controls

The organization shall implement the 21 general controls described in Tables A.1 to A.6.

6 Lottery and gaming specific security and integrity control objectives and controls

The organization shall implement the 90 lottery and gaming specific controls described in Tables B.1 to B.7, if applicable.

Annex A
(normative)

General security and integrity control objectives and controls

The control objectives and controls listed in Tables A.1 to A.6 are mandatory controls under this International Workshop Agreement. They have been derived from ISO/IEC 27001 and extend beyond the requirements of ISO/IEC 27001. The lists in Tables A.1 to A.6 are not exhaustive and a lottery organization may consider that additional control objectives and controls are necessary.

Table A.1 — Organization of security

G.1 Organization of security		
G.1.1 Allocation of security responsibilities Objective: To ensure that security function responsibilities are effectively implemented.		
Type of control		**Control**
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.
G.1.1.2	Security function	A security function shall exist that will be responsible to draft and implement security strategies and action plans. It shall be involved in and review all processes regarding security aspects of the organization, including, but not be limited to, the protection of information, communications, physical infra-structure and game processes.
G.1.1.3	Security function reporting	The security function shall report to no lower than executive level management and not reside within or report to the IT function.
G.1.1.4	Security function position	It shall have the competences and be sufficiently empowered, and shall have access to, all necessary resources within the organization to enable the adequate assessment, management and reduction of risk.
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.

Table A.2 — Human resource security

G.2 Human resource security		
G.2.1 Implementation of a code of conduct Objective: To ensure that a suitable code of conduct is effectively implemented.		
Type of control		**Control**
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.
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.
G.2.1.3	Conflict of interest	The code of conduct shall include statements that employees are required to declare conflicts of interest on employment as and when they occur. Specific examples of conflict of interest shall be cited within the code.
G.2.1.4	Policy on hospitality or gifts	The code of conduct shall include an anti-graft policy also including hospitality and gifts provided by or given to persons or entities with which the organization transacts business.

Table A.3 — Physical and environmental security

G.3 Physical and environmental security		
G.3.1 Secure areas Objective: To ensure that access to production gaming data centres or other systems areas important for the gaming operations are adequately secured.		
Type of control		**Control**
G.3.1.1	Physical entry controls	Physical access to production gaming system data centres, computer rooms, network operations centres and other defined critical areas shall have a two-factor authentication process. Single-factor electronic access control methods are acceptable if the area is staffed at all times.

Table A.4 — Access control to gaming systems

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

Table A.5 — Information systems maintenance

G.5 Information systems maintenance		
G.5.1 Cryptographic controls Objective: To protect the confidentiality, authenticity and integrity of important gaming, lottery and customer related information by cryptographic means.		
Type of control		**Control**
G.5.1.1	Cryptographic controls for data on portable systems	Encryption shall be applied for non-public organization data on portable computer systems (laptops, USB devices, etc.).
G.5.1.2	Cryptographic controls for networks	Encryption shall be applied for sensitive information passed over networks, which risk analysis has shown to have an inadequate level of protection, including validation or other important gaming information, electronic mail, etc.
G.5.1.3	Cryptographic controls for storage	Integrity measures shall be applied for the storage of winning information ticket data and validation information.
G.5.1.4	Cryptographic controls for validation numbers	Encryption shall be applied for instant ticket validation numbers.
G.5.1.5	Cryptographic controls for payment orders	Encryption shall be applied for financial transactions between the organization and a banking institution.
G.5.2 System testing Objective: To maintain the security, confidentiality and integrity of test data.		
G.5.2.1	Test methodology policy and data	The test methodology policy shall include provisions to prevent the use of data created in a live production system for the current draw period and to prevent the use of player personal information.

Table A.6 — Business continuity management

G.6 Business continuity management		
G.6.1 Press media handling and availability Objective: To ensure the protection of organization image and reputation and to counteract interruptions to business activities.		
Type of control		**Control**
G.6.1.1	Press media and personnel handling	The business continuity plan shall include plans to handle the media and personnel during crisis situations.
G.6.1.2	Shareholder or board approval	The organization shall ensure that the board or shareholders of the organization agree to the decided availability requirements.