World Lottery Association

WLA-SCS:2016

Participants' questions fielded by the WLA SRMC during the WLA-SCS stakeholders' workshop held on April 11, 2017 in Zurich, Switzerland

Edition March 2018

About this document

On April 11, 2017, the WLA Security and Risk Management Committee (SRMC) held a stakeholder's workshop in Zurich, Switzerland. The aim of the workshop was to introduce stakeholders to the latest version of the WLA-SCS (WLA-SCS:2016), to compare and contrast it with the previous version of the WLA-SCS (WLA-SCS:2012), and to explain new features in the WLA-SCS:2016. In the course of the workshop, the SRMC fielded a number of questions from the attendees. The participants' questions, and the answers from the SRMC, were recorded and are provided herewith in this document.

General questions related to WLA-SCS

Is it still the case that lottery service suppliers (for example IGT, SGI, Intralot, etc.) can only be certified against WLA-SCS Annex A?

If a supplier is only a provider of services then they certify only to the general controls of Annex A. If the supplier is a provider as well as the operator of the lottery, then they can certify to both Annex A and Annex B.

How shall IWA evolve?
Shall it be reviewed and will the structure change?

The WLA Executive Committee decided two years ago, to make the evolution of the WLA-SCS standard a top priority. The standardization under ISO, of which IWA is an element, which is now work in progress, conveys ample time for development. It is a three to six year process. We are looking toward the possibility of continuing the IWA through 2020 with the option of making the WLA-SCS a full ISO standard. It is a long process but we want to be sure that, as we move forward, we are doing the right thing for the WLA and our standard.

What about outsourced controls, for example the design of scratch tickets done by an external company?
Is this to be considered as "non applicable"?
Otherwise how is this to be controlled?
Is SLA (service level agreement) mandatory?

This is related to the concept of the scope. If you have scratch tickets the responsibility is with the lottery, so this is within the scope of the lottery. As in this case, even if the operation is not being done directly by the lottery, they should have direct control over the operation through a contract. Then the auditor must check that what has been agreed to in the contract is being carried out. Normally, the requirement of the contract will allow for the auditing of the operation to check that the contract is being fulfilled properly. This is the way to organize all that has been outsourced.

Specific questions related to the WLA-SCS (controls)

G.1.1.4	Security function position	*Control* It shall have the competences and be sufficiently empowered, and shall have access to all necessary resources to enable the adequate assessment, management, and reduction of risk.

What kind of evidence is needed to show that the security function is performed by a competent person?

The easiest way would be to ask for the security officers CV. What does one expect to see in the CV of a competent security officer? Perhaps some studies in computer systems, telecommunications, a university degree, CISA certification by ISACA, or maybe ISO 27001 lead auditor certification. You need to check the security officers' professional background to ensure that they have acquired the necessary skills throughout their career. The professional judgement of the auditor is indeed important. If the auditors feels that a security officer's CV is not sufficient they may ask for further evidence.

G.6.2.1	Business continuity plan	*Control* Continuity exercises shall be planned, performed and evaluated in regular intervals to prepare the organization for crisis situations.

Are "dry" desktop exercices towards written continuity plans already enough to fullfill this special requirement or are practical exercices absolutely necessary to execute also already for the first time?

This again is a matter of company policy. The company needs to decide the optimal level of exercises that need to be carried out in the business continuity plan. This requires a risk-based approach. The lottery decides which level of exercises are necessary for their organization. For certification, it is not mandatory to go further than "dry" desktop exercises if that is what fits the organization.

G.6.2.2	Violent situations	*Control* Physical security measures to prevent damage of terror attacks or other threats shall be planned to protect personnel and business processes.

Do we need a lockdown policy?
Is this also for outlets, points of sale?

Again here, it is up to the organization to determine the policies and measures that are required.

Prevent has a double meaning. Do you mean "guard against"?

Prevent means stopping something effectually, in advance, by forestalling action and rendering it impossible. While it is known that making something impossible in safety/security is really "impossible", it conveys a strong sense of protecting human life, intensely!

L.2.4	**Electronic Lottery Draws**
Objective:	To ensure electronic drawing system integrity by physical and logical protection.

L.2.4 assumes that the RNG and drawing algorithm are physically separated in different systems. What if they are not separated and are on the same system? Example: a hardware RNG card installed in the system.

You are not obliged to have the entropy source and the drawing algorithm in the same environment, nor the contrary. L.2.4.2 is applicable both to situations; measures will surely be different from one approach to the other.

L.2.4.1	Physical and logical protection of the technical system	*Control* Measures shall be taken in order to ensure only those authorized have physical access to, and logical protection of, both the Random Number Generator (entropy source) and the drawing algorithm in order to prevent any modification of the algorithm and the entropy source settings. The physical system(s) shall be protected against theft, unauthorized modifications, and interference.

Does "interference" mean protection against electromagnetic interference? E.G. put the system in a Faraday cage? Or just physical interference?

The control is referring to interference by human action, basically those that could change the fair outcome of the electronic drawing system. The SRMC has not considered electromagnetic interference a real threat for the fair outcome. No faraday cage is needed.

L.2.4.3	Electronic draw randomness and integrity verification	*Control* Before deployment, tests and verifications shall be performed by independent parties in order to verify that the electronic drawing system is random. The organization shall document its policy related to after-deployment tests and verifications in order to verify that the random number generator and drawing algorithm is performing as specified.

Is the requirement only to have a policy? Should the auditor assess the suitability of the policy?

Yes, the only requirement is to have a policy, the standard does not require specific after-deployment tests and verifications. While those are good practices in some environments, others might not need those. It is the responsibility of the lottery to define if it needs tests and verification, to what intensity and frequency, as well as the practices of verifying adequate performance, and the expertise of the team eventually performing the tests and verifications. Of course the policy has to be approved at the right organizational level, and of course, the organization must follow what the policy states. The auditor should check to see if the decisions of the company have been made at the right level, and if the policy is being followed. The auditor never has to discuss the content of the decision. As long as the decision has been made at the right level it has to be respected. As said, having a policy is not only paperwork. Once you have the policy, you have to follow the policy. It is not about having a policy paper, it is about following what is written in the policy paper.

Policy is "paperwork", what is required?
Can we share best practices?

Again, a lottery must follow the steps for having a policy approved and the policy has to be followed. So it is not only the policy documentation that counts, but also that the policy must be carried out. Auditors need to check that there is a policy in place, that the policy has been approved at the proper level, and that the policy is being carried out as designated in the documentation.

What qualifies an "independent party" to verify randomness?
For example ISO 17025 accredited test lab with this speciality in scope?
(similar question applies to L.8.1.3 for testing and certification).
What is meant by "independent party"?
Is the four eyes principle ok or should there be real separation of organizational units?

Of course the better the expertise of the "independent party", the better it is for you. The better accreditation of the "independent party", the higher the trust on the verification – better assurance that the good procedures are followed. However, in this case the WLA-SCS is not requesting to have special qualifications for the third party verifying randomness. It is important that this third-party individual (either external or internal) has "no links" whatsoever to the RNG and the algorithm. This includes development, implementation, maintenance, and operations, but excludes verification. The rule of the thumb for separation of duties is that the entity that approves an action, the entity that carries out the action and the entity that monitors the action must be separate. So, four eyes is not enough to ensure separation of duties – it is just a double control. This task can be handled by an external company that is competent in this area. But lotteries are not obligated to go with an external provider. The important thing is that the third-party individual has no ties to the RNG and the algorithm (and the party is functional and hierarchically independent from the electronic draw system teams – systems "care" and operations). To end clarifications, it must be effectively separated from design and production, and this party sets the criteria for verification of randomness and operation.

What is the size of the sample?
What expertise does the independent party need?

Already covered.

Is this applicable to random number generator used in online gaming?
And for the production of scratch cards?

In relation to the online gaming, the requirement to have a policy stands. This control does not apply to scratch lottery.

L.3	Retailer security	
L.3.1	**Recruitment and set-up**	
Objective:	To ensure that only approved people, operating in approved locations, are accepted as retailers to sell the organization's products on and off-line.	
L.3.1.1	Retailer contract	*Control* Retailers shall be engaged under the terms of an agreed contract.

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

Shall we also audit the retailers?

Should the retailers be external providers, it has to be checked that the lottery takes due care of the control of the outsourced operations, as already said. Most lotteries do not operate a retailer network with their own staff, so it has never been considered as a requirement to audit the full retailer network. Most lottery retailer networks are vast, with up to 30-thousand points or more. It is impossible to audit all those retailers (typically for such situations a sampling method is followed). The auditor must check that the retailers operate under a contract (this verification is done at the lottery) and that the lottery specifies the security environment the retailer is required to operate (this verification is also done at the lottery).

Usually, to gain assurance, auditors like to understand and perceive how retailers operate. They typically go to one retailer near the lottery, purchase a few products (such as scratch tickets), they check the scratch tickets and have one or two questions for the retailer. Typical questions would be: "Has the lottery provided security requirements/procedures for you?" and "How are you being followed up by the lottery?" Usually the auditor asks the lottery how they follow up with the retailers if there has been a security incident.

So, the WLA-SCS is not specifically requesting retailer audits, but the auditor can wish to talk to a retailer in order to verify the assertions of the lottery related to their obligations. Certainly the lottery is not obliged to take the auditor to the retailer. However, the auditor can request to see a retail operation in the course of an audit. If the auditor requests this of the lottery, it is recommended to facilitate it. Keep in mind that it is up to the auditor how to verify compliance within the scope of the audit.

L.6 Digital sales channels and interactive services

Is this covering traditional online gaming systems, that is, central based systems? Those also work on a digital basis – vs an analogic basis …

Digital sales channels refer to channels where the player is the "owner" of the remote device. L.6 is fully related to remote purchases (such as draw lotteries) and interactive gaming (such as internet real-time scratch cards).

L.6.1.6	Generation and storage of logs	*Control* Logs shall be generated on each sensible system component in order to monitor and rectify anomalies, flaws and alerts. All logs shall be stored in order to be presented as evidence in the jurisdiction the lottery operates.

What does "evidence" mean in regard to fulfilling this requirement?

The requirement behind this control is that the lottery has to be able to provide to the authorities evidence in the case of an investigation. This is not about providing evidence to an auditor during an audit. This requirement is dependent on the regulations within the lottery's respective jurisdiction. Auditors should always keep in mind that the law, in all cases, takes precedence over the standard. The objective here is to protect the gaming and player data. In relation to how long and how much evidence has to be stored, the main driver here is the applicable regulation. So logs have to be stored and remain available upon request of the authorities. Certainly auditors can ask for information regarding the legal obligations and how those are fulfilled.

L.6.1.7	Security testing	*Control* There shall be appropriate security testing on major system changes. Regular intrusion testing that attempts to identify and exploit vulnerabilities or other system weaknesses shall be performed.

Shall this be performed by the lottery?
We have a specialized company doing it for us.

It can be performed in house or externalized. The WLA-SCS is not imposing any specific way, it only requires that testing is done – certainly by competent persons.

L.6.2.3	Players exclusion	*Control* There shall be an established process for excluding players in accordance with local applicable laws and/or internal procedures.

Does "Players exclusion" refer only to money laundering and fraud or does it also cover to age restriction and responsible gaming?

The main objective of all the controls in L.6.2 is to protect the player and to fight fraud and money laundering. So it should be clear that control L.6.2.3 refers to responsible gaming and age restriction as well as money laundering and fraud. Having said that, we need to emphasize that the WLA has a Responsible Gaming Framework (WLA-RGF) that would explicitly address the exclusion of underage players

or the exclusion of players due to questionable playing behavior. Here, the WLA-SCS's main focus is to point to the place where Responsible Gaming controls must be implemented. However, it is true that player protection is furnished, from different angles, by both the security practices of the WLA-SCS and by the responsible gaming practices of the WLA-RGF. This is one of the areas where the two standards have common objectives. On the other hand, the WLA-SCS also takes care of compliance with age restriction regulations whenever applicable, would the organization be following the WLA-RGF or not.

L.6.2.4	Multiple payment instrument holder	*Control* There shall be an established procedure for assuring the match of ownership between the payment type holder and the player account holder.

What happens if bank secrecy laws prohibit the execution of this control?

Once again, law takes precedence over the standard. If bank secrecy laws prohibit the execution of this control, then the control is not applicable.

Who can pay into the player account?
Is it only the account holder or can other parties pay into the account?

The control has to be understood in light of the regulations in the lottery's jurisdiction. In some jurisdictions it is expressly forbidden for anyone other than the account holder to make payments into the account. There are other jurisdictions that have no regulations on this issue. Still others consider that payments made by members of the same family are indistinguishable. Different levels of formality are required for a person acting officially in name of another. Again, law takes precedence over the standard. The auditor should apply this control in accordance with the laws of the jurisdiction in which the audited lottery is operating.

L.6.3.2	Game approval and modification	*Control* An approval procedure shall be defined to validate that every new game and relevant modifications on the digital are controlled. Final game design shall be formally approved through a process involving the Security Function.

The security function has no role in approving game modification.

This control has not changed since 2012. Of course the security function has to ensure that game changes do not affect the residual risk in an uncontrolled manner, and it must evaluate that removing existing, or to be modified, controls do not have a negative or unacceptable impact on security.

L.6.4.1	Data collection	*Control* Collection of sensitive data directly related to payment shall be limited to only the data strictly needed for transaction.

What is referred to as "sensitive"? is it based on local law?

According to the ISO 27001, one must create an information classification scheme and designate on that scheme what is considered sensitive data. This is what is reflected here in this control. You need to refer to the information classification scheme that has been created in accordance with the ISO 27001.

L.6.4.3	Payment service approval	*Control* The organization shall verify that the payment service ensures the protection of the player data, including any personally identifiable information given by the player or payment related data.

The payment service is subcontracted, then this control cannot be fulfilled.

This activity is within the scope of the lottery. As already explained elsewhere, the control of providers is absolutely mandatory. That the lottery is not performing an activity with its own staff and resources does not imply that the lottery is not responsible; so, the lottery must control the activity.

L.7 Sports betting

Are virtual games and events – such as e-football, or dog races to be considered in "sports betting"?

Without entering in any kind of discussion in relation to the nature of sports, the standard is focused on real human sport games. So the answer is no, currently neither virtual events nor dog racing are covered under L.7. This could change in the future, but for now, if one of the operations you are auditing offers betting on such events you would not include it in L.7.

L.7.1.3	Authorized betting options list	*Control* Maintain a list of betting types per game type. Specific procedures shall be implemented in the case of nonprofessional events.

Could you specify, with examples, what the term "nonprofessional events" is in reference to?

In football, for instance, the lower-level leagues pose a greater risk in terms of match-fixing. For example, generally for the football national cup bets are only offered at a certain level. Amateur teams are excluded as the danger of corruption at that level is high and usually unacceptable. These would be considered nonprofessional events. Generally, the regulatory authorities detail which nonprofessional sports and which type of nonprofessional events are authorized for betting and why.

What about "friendly matches"?

Friendly matches also pose a degree of risk. While L7.1.3 is not requesting any specific procedures, the organization should establish rules concerning their use.

L.7.3.1	Results for completed events	*Control* There shall be a policy for the confirmation of results based on qualified and approved sources, before publicly announcing results and declaring winners.

How does one evaluate what is a "qualified and approved" source?
What evidence does one need to collect in order to prove it?
Is checking the results on official sport website enough?

If the laws and the regulator do not define what a "qualified and approved" source is, then it is up to the operator to do so. What the WLA-SCS means here by a "qualified and approved" source is a source that can provide reliable and timely results, and that has been so designated and approved by the organization. It is important to ensure that the results for all the events come from reliable and reputable source. It is up to each betting operator to be connected with a good source and to be able to document that the source is reliable and reputable.

What evidence does one need to collect in order to prove it?

First of all, that is not the concern of the auditor. The selection of the source is a professional decision made by the top management. The auditor has only to check that a system is in place and that it has been cleared by the top management.

L.7.3.2	Results records	*Control* A backup record of all results shall be kept and identified as a critical asset.

How long must the records be retained?
We get the results from XYZ.

As already explained elsewhere, retention time depends on the legal obligations of the lottery. While your provider guaranties the availability of data, there is not any need that the lottery keeps by itself the data.

L.7.4	**Monitoring for fraud and money laundering**
Objective:	To ensure actions to minimize the risk of fraud and/or money laundering.

What to do if there is no local law for this?

In the absence of local laws governing fraud and money laundering, the lottery should establish and document its own policy and actions to minimize the risk of fraud or money laundering. Events of fraud and/or money laundering are not good for the lottery, even if no legal requirement applies. Important international references can be taken from UN conventions and UN Security Council resolutions and the FATF Recommendations, as well as from other countries national or supranational regulations.

L.7.5.3	Courtsiding prevention mechanisms	*Control* Ensure customer protection and fraud/integrity protection through the provision of a safety mechanism to account for delay in live pictures.

What are those safety mechanisms?

Note that in some jurisdictions courtsiding is legal and in others not. Mechanisms? Such as controlling which feeds have delays, to introduce delays of 5 to 10 seconds to live bet processing, two clicks approaches (as a way to introduce a delay) and to cap bets. Alternatively bets could be offered in relation to events happening not closer that some seconds to the made bet. Monitoring is also an effective measure, so, when courtsiding is illegal suspicious bets could be rejected. When courtsiding is legal, tighter controls and better feeds must be used. In case of unacceptable risk due to a poor link, the event should not be retained.

L.7.6	**Duties separation and internal control**
Objective:	To avoid internal collusions.

L.7.4.4	Cash payment of winnings	*Control* A procedure shall be established specifying thresholds of payment and methods of collection.

L.7.4.6	Deposit monitoring	*Control* Establish a level above which deposits of a certain size are monitored.

Those requirements are redundant, are duplicated from other sections.

Controls are associated by kind of games, as not all lotteries and gaming organizations operate the same games. Depending on the games operated, for some organizations some sets of controls are non-applicable. Duty separation is a need for different kind of games, so those are reflected in the different sections wherever needed.

L.7.6.2	Corporate betting policy	*Control* There shall be an internal policy addressing employees' rights to play.

How to control the employees?
Is it enough to have a policy or should there be measures to check?
By the way, it is hardly possible to verify if they register under a fake identity with another account number.

It is important that sports betting operators have a policy in place that outlines their employees' right to bet, especially if employee betting is forbidden by law. If employee betting is forbidden by law and/or if the policy of the betting operator designates that employees are forbidden to bet, there should be a system in place to ensure that this does not happen. If of course an employee registers under a fake name (when this is allowed by the regulation), the lottery cannot control them – lotteries are not the police. But what is certain is that employees, registering under a fake name will eventually be caught and investigated for fraud – especially when cashing

prizes. So, the importance of the policy is to ensure that employees know they are/are not allowed to play, awareness and training is very important here. Besides, the organization will decide on which measures can be adopted to check compliance (such as cashing prize checks).

L.8 Interactive Video Lottery Terminals (VLT)

L.8.1.3	VLT game certificate	*Control* Dedicated games for VLT shall be tested and a certificate to provide evidence of integrity has to be maintained/issued.

What precisely is meant by "dedicated" games for VLT?
What is a VLT?

A VLT is video terminal, located usually at points of sale, that allows customers to play to VLT-dedicated games. VLTs are directly operated by the players in a pre-sential manner – not remote. That means that a VLT is dedicated mainly to its own games. It is not an access terminal per se in the sense of a smartphone, PC or tablet/Ipad – all of which allow players themselves to connect and to purchase/play the digital sales channels and interactive services gaming product offerings of the lottery. This focuses what games dedicated for VLTs are.

Other points and observations

There were some other points and observations received, not directly related to clarifications or understandings of the WLA-SCS. Those have been duly noted by SRMC and will be included in the SRMC work program for evaluation.

World Lottery Association

WLA Security Control Standard

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

WLA-SCS:2016