TECHNICAL AND OPERATIONAL NOTE ON BIENNIAL AUDITS OF GAMBLING TECHNICAL SYSTEMS. (version 2).

1. Document objective

The 12th Article, "Technical gambling systems audits" of Royal Decree 1613/2011, of November 14th, which develops Law 13/2011, of May 27th, on the regulation of gambling, regarding the technical requirements of the activities of the game, states that:

1. Technical gambling systems must be audited every two years. The audit, whose costs shall be borne by the operator, may be conducted by the Directorate General for the Regulation of Gambling or by an entity proposed by the former from among those entities permitted to authorise and certify technical gambling systems and being distinct from the entity that conducted the previous authorisation and certification report of the operator's technical gambling system.
2. The first audit shall be conducted within six months following the two year expiration date counted from the granting of authorisation. Subsequent audits shall also be conducted within six months following the two-year expiration date.

In the event that the audit is not conducted by the Directorate General for the Regulation of Gambling, the positive report resulting from the audit must be submitted for the assessment of said Directorate.

3. If the positive audit report is not submitted to the Directorate General for the Regulation of Gambling within the prescribed time, the Directorate will suspend the activity of the operator on a provisional basis and will commence the relevant proceedings for revoking the specific licence.
4. On the basis of sanction proceedings or of actions prior to such proceedings, the Directorate General for the Regulation of Gambling may order the auditing of the gambling systems of the presumed infringing operator. The audit may be conducted by the Directorate General for the Regulation of Gambling or by an entity appointed by the former from among those entities permitted to authorise and certify gambling systems and being distinct from the entity that conducted the previous authorisation and certification report of the operator's gambling system.
5. The Directorate General for the Regulation of Gambling shall issue the specific provisions or instructions considered necessary for conducting the audit."

The objective of this note is to set out the technical and operational instructions for performing the audits. This document describes the objective of the audit, the scheduling of the biennial audits during the validity of the licences as well as the format and minimum content of the report to be submitted to the Directorate General for the Regulation of Gambling (DGOJ).

2. Changes Control

Date	Version	Description
2015/04/01	1.0	Versión inicial.
2017/05/03	2.0	A number of requirements are removed from the scope of the audit and certain clarifications are introduced.

3. Index

4. Purpose of the audit

The biennial audit of the technical gaming system is aimed at verifying the technical and organizational adequacy of the requirements established in articles 17th and 18th of Law 13/2011, of May 27th, regulating the game, with special reference to:

- The existence and appropriate operation of the internal control procedures for the activity. The implementation of a procedure involves a task manager and an audit record. The correct implementation of each procedure and the effective performance of the different tasks assigned to each person taking part in the procedure, must be audited. The record associated with the procedures and its correct and regular updating must be audited.
- The compliance with the requirements regarding records, traceability and storage of information. With regard to the obligations stipulated in the regulations relating to information storage, the following must be verified: the existence of records, their storage for the minimum period established under the regulations and the correct updating of records through the relevant procedures for such a purpose.
- The existence and correct functioning of security policies and procedures. The purpose of the security audit is to verify the correct operation of security policies, procedures and instructions. Therefore, the auditor must identify and review all indications that show the proper implementation of each procedure and control put in place within the operator's established framework for information security management.
- Verification of the random nature of the gambling systems and game logic. The random number generator in operation must be checked that it matches the previously certified generator. Furthermore, all controls and procedures relating to the proper functioning of the game logic must be audited.

5. Performance of the audit

Technical gambling systems must be audited every two years by a certified entity from among those entities permitted to authorise and certify technical gambling systems and which is not the entity that conducted the previous authorisation and certification report of the operator's technical gambling system.

Given that authorisation is valid for a period of ten years, the following audit cycle is established[1]:

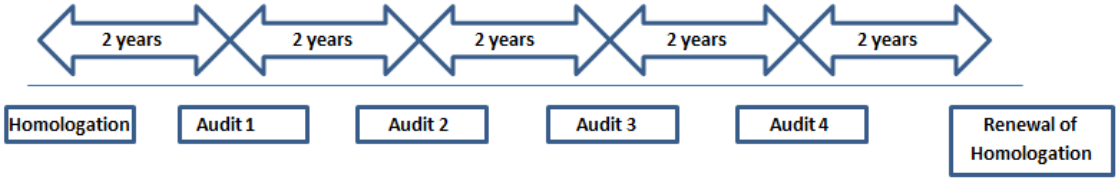

Illustration 1 - Audit Cycle

The first audit shall be conducted within six months following the two-year expiration date counted from the initial authorisation for the specific licence or from the decision date on change management authorisation whose scope encompasses the entire technical gambling system of the operator. From then on, subsequent audits shall be conducted every two years, within a six-month grace period.

The time limits established for conducting each and every audit shall be determined by the date indicated in the previous paragraph. In other words, the date on which an audit is conducted does not determine the date for subsequent audits.

The audit will be carried out on the complete technical system used by the operator for the development of its activity in the framework of **Law 13/2011**, of May 27th, on the regulation of gambling. In order to homogenize processes and combine efforts, the operator may include under the scope of the first audit all of its licenses, regardless of whether some of them were subsequently approved.

The security audit must be conducted by security-certified entities and the functionality audit must be conducted by entities certified in gambling software.

[1] An audit cycle is the set of compulsory biennial audits (4 in total) for one authorisation period (10 years)..

6. Basic form and content of the audit report

The audit report will be structured in the following sections:

In the following sub-sections, the minimum content for each of these sections is detailed.

1. Identification of the audit

The first page of the report will detail the following:

1. Report type: "Biennial audit report on technical systems for gambling" shall be stated.
2. Identification code of the report: The identification code of the report shall be unique, allowing the report to be referred to unambiguously and distinct from any other report issued by the auditor. Any time that the auditor modifies a report, a new identification code will have to be generated and the changes to the audit report must be identified.
3. Recipients of the audit report.
4. Details identifying the auditor.
5. Details identifying the audit team.
6. Details identifying the report's signatory on behalf of the auditor.
7. Dates on which the audit work was performed.
8. Audit scale according to man hours.
9. Publication date of the audit report.

2. Description of the audit's subject matter

The subject matter of the audit shall be the actual technical gambling system employed by the operator for carrying out and operating gambling activities covered by the relevant licence in relation to the procedures, processes, arrangements and security measures in effect.

In describing the scope of the audit's subject matter, the following shall be enumerated:

- **Gambling licenses** within the scope of the audit.

- **Software providers** under the scope of the audit.

  For this purpose, the following format will be used:

License	Software porvider

- **Data processing centres (CPD) where the technical gambling system is located, in the following format:**

CPD	Address	City	Country	Type	Business name of the hosting provider

The fields "street", "number", "city" and "country" refer to the physical location of the CPD. The "type" field indicates the hosting method of the CPD and must match one of the following: "hosting", "co-location" or "own".

The field "business name of hosting company" only requires filling out if the "type" field is either one of: "hosting" or "co-location".

Both the certification report code certifying the CPD and the date of authorisation must be included.

- **Software components** used in the technical system for carrying out and operating the gambling activity covered under the relevant licence, expressly stating the manufacturer, product name and version. In all cases the data capturer and storage regarding the components must be recorded.

The components shall be enumerated in the following format:

File Name	Version	Logical location	Physical location	Fingerprint	Producer	Product name

The logical location refers to the server and / or servers that are running the file.

The physical location refers to the CPD in which the file is physically located.

Fingerprint identification should identify the type of function / algorithm used to calculate the footprint (MD5, SHA-1, SHA-256, SHA-512, etc.).

3. Executive summary of the audit

The purpose of the executive summary of the audit report is to present high-level information in relation to the audit and its most relevant aspects. Such information comprises the following sections:

A. Overall classification

The overall classification table presents the overall classification for the compliance of each sector of audited requirement in the following format:

Sector	Overall Classification
Security requirements	
Functionality requirements for General Licences	
Functionality requirements for Specific Licences	

Under Overall Classification, if no non-conformities have been identified in relation to the requirements of each sector, Compliant is stated; otherwise, Not compliant is indicated. In the event that a certain sector is not within the scope of the audit report, Not applicable shall be stated.

B. Executive Comment

Under the executive statement section, the audit team describes its overall impression on the audited technical gambling system. It presents its most important conclusions on the system and identifies examples of its main strengths and weaknesses.

4. Continuous Improvement

The continuous improvement section includes an analysis and follow-up of the improvable elements identified during the auditing process. As a result, this section is divided into two sub-sections: the first is directed towards suggesting actions for improving on such elements and their causes, the second is aimed at reviewing the improvement action plan proposed in the preceding audit.

Improvable elements are features that, despite not entailing non-conformity of a requirement, could become one or point to an impairment in the effectiveness of the measures established by the operator for complying with the requirements.

A. Improvement action plan

This section must include the analysis on the root cause of each improvable element identified during the audit along with the suggested improvement actions that the operator shall carry out to correct said points and their causes.

The format to be used is as follows:

Improvable element number	
Requirement	
Improvable element	
Root cause	
Proposed improvement action(s) propuestas	

The Improvable element number is a sequential number for the improvable elements identified in each audit report.

Requirement refers to the requirement related to the improvable element and identifies the applicable regulation and article.

The Improvable element field describes the features of the improvement identified for the technical gambling system.

The Root cause field must include the conclusions of the analysis directed towards identifying the underlying reason(s) of the improvable element.

The Improvement action(s) field must include the list of actions to be performed for correcting the issues that make up the improvable element and its root causes.

B. Review of the improvement action plan

This section must include details on the follow-up of the improvement action plan incorporated in the previous audit report.

The following format shall be used for each one of the improvable elements identified in the previous report:

Audit	
Improvable element number	
Requirement	
Improvable element	
Root cause	
Proposed improvement action(s)	
Closed (Y/N)	
Observations	

The Audit field shall state the code of the audit report in which the mentioned improvable element was identified along with the report's date.

The Closed field states whether or not the audit team considers the improvable element and its root causes to have been corrected.

The Observations field includes details on the indications identified by the audit team, which shows the correct implementation of the improvement plan proposed by the previous audit. Also included in this field will be details of modifications made if new root causes have been identified or if improvement actions not identified in the preceding audit report have been carried out.

All other fields shall have the same content as included in the original presentation of the improvable element in the previous audit report.

Please take into account that section B: "Review of the improvement action plan" is not necessary in the first audit conducted.

5. Description of the auditing environments differing from those used by the operator in carrying out the gambling activity

In the event that particular verifications of the technical gambling system are conducted under an environment different to that employed by the operator in carrying out and operating the gambling activity covered by the licence, the auditor must describe the different environments used in this section.

For each different environment, the link between the conducted verification and the given environment shall be stated.

6. Compliance details on the audited requirements

This section shall include:

- A summary table of the compliance level in each audited area.
- Compliance details on every audited requirement. The possible classifications for each requirement are: "Compliant", "Not compliant" or "Not applicable".

For all requirements referring to the duty of operators to have in place a procedure, the audit must look into the actual existence and implementation of said procedure.

The following sub-sections elaborate on the content.

A. Summary table of the compliance level by area

The overall classification table presents the compliance classification for each area audited in the following format:

Sector	Area	Audited	Overall Classification
Security	Security policy		
	Risk analysis and management		
	Organisation of information security		
	Security of communications with participants		
	Protection of human resources and third parties		
	Physical and environmental protection		
	Management of communications and operations		
	Access control		
	System purchase, development and maintenance		
	Management of security incidents		
	Change management		
	Plans for preventing information loss		
	Business continuity management		
	Vulnerability analysis and penetration testing		
General Functionality	Responsible Gambling		
	Contract, Acceptance, copy and amendment		
	User registration and exclusion checks		
	Gaming account, amounts paid and collected		
	Deposit limits		
	Records and traceability		
	Terminals and user sessions		
	Communication channels		
	Internal control system (SCI)		
Specific functionality	Licences		
	Relationship with participants		
	Return percentage and prize tables		
	Random number generator (GNA)		
	Game logic		
	Records and traceability		
	Terminals and user sessions		
	Communication channels		
	Behaviour in relation to technical faults		
	Real-time gambling		
	Various features		
	Roll-over jackpots		
	Internal control system (SCI)		
	Record of session configurations for online slot-machine gambling		

YES or NO is indicated in the *Audited* column.

The *Overall Classification* column must only be completed for those areas that are audited. *Compliant* shall be the term used where no non-conformities are found in relation to the requirements of each sector, otherwise, *Not compliant* shall be used.

B. Compliance details on the security requirements

The form for the security audit to follow is as described in Appendix VII of the RES_INF, with the following provisos:

The purpose of the security audit is to verify the correct operation of security policies, procedures and instructions stipulated in the regulations. Therefore, the auditor must identify and review all indications that show the proper implementation of each procedure stipulated in the regulations. The review must include the effective execution of the different tasks assigned to each person taking part in the procedure, along with checking that the procedure's audit trail has been correctly updated at the appropriate frequency.

Concerning the duties stipulated in the regulations relating to information storage, the following must be verified: the presence of the relevant records, their storage for the minimum period established under the regulations and the correct updating of records through the relevant procedures for such a purpose.

In the Classification column, if no non-conformities have been identified in relation to the requirement, *Compliant* is stated; otherwise, *Not compliant* is indicated. If a particular requirement does not fall within the scope of the audit report, *Not applicable* shall be noted.

If certain requirements can endorse by an ISO 27001 certificate and done so, the classification, *Endorsed*, shall be used and "ISO 27001" shall be noted under *Observations*.

Furthermore, it shall be necessary to document the following situations in the Observations field:

- The reason for the requirement being "*Not applicable*".
- In the occurrence of any incidents even though they had been subsequently rectified.

Special attention must be given to the essential security areas requiring verification in a particular audit of an audit cycle.

The following table summarises the security areas requiring examination in a given audit. The abbreviations, A1, A2, A3 and A4, refer to the particular audits respectively taking place two, four, six and eight years after the initial authorisation.

Area	A1	A2	A3	A4
Security policy	YES		YES	
Risk analysis and management	YES	YES	YES	YES
Organisation of information security		YES		YES
Security of communications with participants	YES		YES	
Protection of human resources and third parties		YES		YES
Physical and environmental protection		YES		YES
Management of communications and operations		YES		YES
Access control	YES		YES	
System purchase, development and maintenance		YES		YES
Management of security incidents		YES		YES
Change management	YES	YES	YES	YES
Plans for preventing information loss		YES		YES
Business continuity management	YES		YES	
Vulnerability analysis and penetration testing	YES	YES	YES	YES

In response to an organizational criterion, it is possible to start the audit cycle in A2 instead of A1. This is mainly due to the fact that for a significant number of operators, the first audit of the singular license of random machines coincides in time with the second audit of the other licenses of which it is the holder. In this sense, it is possible that for a given provider or for a particular license, the first security audit to be executed is the one corresponding to the scope of audits A2 and A4.

C. Compliance details on the general functionality requirements

As indicated above, the audit of general functionality requirements focuses on reviewing the correct implementation of control procedures, the preservation of information and the records established in the standard.

Note that for the purpose of a better understanding by the reader, the structure of the *" Guidelines on technical functionality requirements v2"*, published on the website of the DGOJ has been maintained, with the following exceptions:

- The general functionality requirement verification questionnaire is a subset of the set of requirements listed in the guide.
- • The following new issues for auditing have been included:
    - In relation to the "Internal Control System" area, the requirement established in section 5.1.13 of Annex I of RES_TEC "Conservation of information of the ICS" is included.
- The column *"Requirement"* transcribes the requirement established in the standard, object of the audit.
- The purpose of the *"Auditor's Tasks"* column is to clarify the tasks to be performed by the auditor.
- In the *Qualification* field, it is indicated *conformed* if no non-compliances were identified in the requirement, or *not conformed* otherwise. If the requirement is not applicable to the audit report, it will be indicated *Not Applicable*.
- In addition, it will be necessary to document in the field of Observations, field to be completed by the auditor, the following situations:
    - The reason why the requirement could be qualified as 'Not applicable'.
    - When there have been incidents, although they have subsequently been corrected.

The general functionality requirements verification questionnaire, which should be included in the audit report with the results of the audit, is listed in Annex I of this note.

D. Detail of the fulfillment of the requirements of singular functionality

As noted above, the audit of unique functionality requirements focuses on reviewing the correct implementation of control procedures, the maintenance of the information and records established in the standard and the verification of the randomness of Game systems and game logic.

Note that for the purpose of a better understanding by the reader, the structure of the "Technical Requirements Guide for Functionality v2", published on the website of the DGOJ has been maintained, with the following exceptions:

- In response to an organizational criterion, the questionnaire includes the requirements of all individual licenses. This should not be confusing, since each audit should follow the requirements that apply in the licenses that have been included under the scope of the audit.
- The unique functionality requirements verification questionnaire is a subset of the set of related requirements in the Guide for all single licenses.
- The following new areas have been included:
    - Registration of the configuration of the session for the game of chance machines (applicable only to the audit of the Single License of machines of chance)
    - In relation to the "Random Number Generator" area, a new requirement with description "GNA homologation" is included. The scope of this requirement is to audit that the fingerprint of the GNA is the same as the last homologation report.
    - In relation to the "Internal Control System" area, the requirement established in section 5.1.13 of Annex I of the RES_TEC "Conservation of information of the ICS" is included.
- The column "Requirement" transcribes the requirement established in the standard, object of the audit.
- The purpose of the "Auditor's Tasks" column is to clarify the tasks to be performed by the auditor.
- In the Qualification field, it is indicated conformed if no non-compliances were identified in the requirement, or not conformed otherwise. If the requirement is not applicable to the audit report, it will be indicated Not Applicable.
- In addition, it will be necessary to document in the field of Observations, field to be completed by the auditor, the following situations:
    - The reason why the requirement could be qualified as 'Not applicable'.
    - When there have been incidents, although they have subsequently been rectified.

The singular functionality requirements verification questionnaire, which should be included in the audit report with the results of the audit, is listed in Annex I of this note.

7. Description of the documentation attached to the audit report

The audit report issued by the certification body shall be accompanied by the following documentation:

Full documentation used to demonstrate compliance with audited requirements, which will be collected in a folder called "Documentation".

Within the documentation submitted, as a minimum and without limitation, the following should be present:

- Results reports of penetration tests and vulnerability analysis performed.
- In case of compliance with safety requirements by organizations that have a certified information security management system based on the requirements of ISO 27001:
  - Copy of the current certificate.
  - Report of the last certification audit.
  - Applicable Statement of Applicability (SoA).

- Evidence of the evaluation of audited requirements. They shall be grouped together in a folder called 'Technical requirements'.

7. Points of improvement and non-conformities

In case of non-conformities detected during the audit, the necessary measures must be taken to correct them and make a risk assessment associated with each case. If in the course of the audit and prior to the issuance of the audit report, the identified disagreement is corrected, it should be noted what happened in the report. In case that its correction is postponed to the issuance of the report, the report must include an estimated date for the implementation of the necessary changes. The operator must submit a second version of the report once the non-conformities have been corrected.

The improvement points identified should be dealt with as detailed in section 6 of this document. Unlike non-conformities, improvement points do not require the issuance of a new version of the audit report, but their revision is postponed to the next audit.

8. Incompatibility between certification bodies

Article 12 Audit of the technical gaming systems of Royal Decree 1613/2011, November 14th, which develops Law 13/2011, of May 27th, regulation of the game, regarding the technical requirements of the activities of the game, states that:

"The audit may be carried out by the General Direction of Management of the Game or by the entity designated for this purpose among those recognized for the approval and certification of the game systems and that will be different from the entity that had performed the last audit of the operator's game systems."

In accordance with the previously established:

The certification body performing the audits may not have participated in the initial certification or certification of substantial changes to the audited platform.

The functionality and security audits are independent and therefore, the incompatibility of the functional certification entities is independent of the incompatibility of the security certification entities.

The same certification body may perform all audits, every two years, provided that it has not participated in the certification processes of said platform.

In the case of a complete change of platform, the laboratories that certified and / or audited the previous platform are not subject to the rule of article 12: they could audit the new platform, provided they have not participated in the certification of the platform to be audited.

9. Form of presentation of the audit report

The audit report should be presented only in electronic format through the electronic site of the DGOJ, of the process called "Generic Communications to the DGOJ" available in the section of the "Procedures and Services / General Utility" section, with the following data:

- Unit: S.G. Game Inspection
- Subject: Biennial audit

10. Normative context and abbreviations used

- **Law 13/2011**, of May 27th, regulating the game (LEY_RJU).
- **Royal Decree 1613/2011**, of November 14th, which develops Law 13/2011, of May 27th, regulation of the game, regarding the technical requirements of the activities of the game **(RD_TEC).**
- **Royal Decree 1614/2011**, of November 14th, which develops the Law 13/2011, of May 27th, regulating the game, with regard to licenses, authorizations and registrations of games **(RD_LIC).**
- **Order EHA 3079/2011**, of November 8th, which approves the basic regulation of "Other matching bets" **(OM_OAC).**
- **Order EHA 3080/2011**, of November 8th, which approves the basic regulation of sports betting of counterpart **(OM_ADC).**
- **Order EHA 3081/2011**, of 8 November, which approves the basic regulation of the mutual sports bets **(OM_ADM).**
- **Order EHA 3082/2011**, of November 8th, which approves the basic regulation of counterparty betting **(OM_AHC).**
- **Order EHA 3083/2011**, of November 8th, approving the basic regulation of mutual horse betting **(OM_AHM).**
- **Order EHA 3084/2011**, of November 8th, which approves the basic regulations of the competitions **(OM_CON).**
- **Order EHA 3085/2011,** of November 8th, which approves the basic regulation of the game of roulette **(OM_RLT).**
- **Order EHA 3086/2011**, of November 8th, which approves the basic regulation of the point and bench game **(OM_PUN).**
- **Order EHA 3087/2011**, of November 8th, which approves the basic regulation of the bingo game **(OM_BNG).**
- **Order EHA 3088/2011**, of November 8th, approving the basic regulation of the Black Jack game **(OM_BLJ).**
- **Order EHA 3089/2011**, of November 8th, approving the basic regulation of the game of poker **(OM_POQ).**
- **Order EHA 3090/2011**, of November 8th, which approves the basic regulation of the type of games called "Complementary Games" **(OM_COM).**
- **Order HAP / 1370/2014**, of July 25th, approving the basic regulation of the game of chance machines **(OM_AZA).**
- **Order HAP / 1369/2014**, of July 25th, approving the basic regulation of cross betting, and amending various ministerial orders approving the basic regulation of certain games **(OM_ACX).**
- **Order HAP/1995/2014**, of October 29th, 2014, approving the list of bases that will govern the call for general licenses for the development and exploitation of gambling activities of Law 13/2011, of May 27th, game regulation **(OM_PLG).**
- **Resolution 2014, October 6th,** approving the data model of the information monitoring system corresponding to the game operations records **(RES_MOD).**

- **Resolution 2014, October 6th,** approving the provision that develops the technical specifications of game, traceability and security that must comply with technical systems of game of non-reserved nature subject to licenses granted under the protection of Law 13/2011, of May 27th, regulating the game **(RES_TEC).**
- **Resolution of October 6, 2014**, of the General Direction of Game Management, which approves the provision that establishes the model and content of the final certification report of the technical systems of the gaming operators and develops the procedure Change management **(RES_INF).**

11. Service of consultations and doubts of the DGOJ

In case of doubts, the attention of consultations is made through the electronic headquarters of the General Direction of Game Management and through the mailbox of dgoj.control@minhafp.es according to the following instructions:

To: dgoj.control@minhafp.es

Subject: "BIENAL AUDIT CONSULTATION" and a title for the consultation.

Body of the email:

- Identification of the operator (s) or certification body (s) on behalf of whom the consultation is carried out.
- Identification of who performs the consultation.
- Consultant.

The consultations and doubts will be answered in Spanish or English, as far as possible.