AUTORITÉ NATIONALE DES JEUX

NATIONAL GAMING AUTHORITY

FRENCH REPUBLIC

TECHNICAL REQUIREMENTS FOR THE CERTIFICATION OF LICENSED GAMING OPERATORS OR HOLDERS OF EXCLUSIVE RIGHTS

IMPORTANT WARNING: Though the present English translation has been conducted with utmost care for ease of use by technical teams of the gaming and betting operators not proficient enough with French language, the operator's attention is drawn to the fact that the French version of the document is the only legally binding one.

Summary

In accordance with Article 23 of Law No 2010-476 of 12 May 2010, licensed operators or holders of exclusive rights are subject to a certification procedure (after 6 months and annually).

Un régulateur au service d'un jeu sûr, intègre et maîtrisé

Table of Contents

I General description

I.1 Reminder of legal and regulatory obligations

Article L.320-3 of the Internal Security Code:

' The objective of the State's gambling and betting policy is to limit and regulate the supply and consumption of games and to control the operation thereof to:

1. Prevent excessive or compulsive gambling and protect minors;

2. Ensure integrity, reliability and transparency of gaming operations;

3. Prevent fraudulent or criminal activities as well as money laundering and the financing of terrorism;

4. Ensure the balanced operation of the different types of games to avoid any economic destabilisation of the sectors concerned."

Article 23 of Act No 2010-476 of 12 May 2010 on the opening-up to competition and regulation of the online gambling sector:

'I. – Any undertaking licensed as an online games and betting operator provided for in Article 21 shall comply with the obligations laid down in Articles 15 to 19.

II. – Within six months from the date of entry into operation of the medium provided for in Article 31, the online games or betting operator shall submit to the National Gaming Authority a document certifying the certification it has obtained, which shall relate to its compliance with the obligations relating to Articles 31 and 38. This certification shall be carried out by an independent organisation selected by the operator from a list drawn up by the National Gaming Authority. The cost of this certification is borne by the online gaming or betting operator.

III. – Within one year from the date of obtaining the license provided for in Article 21, the online games or betting operator or the operator holding exclusive rights shall transmit to the National Gaming Authority a document certifying the certification it has obtained. This certification shall cover compliance with all the technical requirements laid down by the Authority with regard to the integrity of gaming operations and the security of information systems. It shall be carried out by an independent organisation selected by the operator from the list mentioned in II. The cost of this certification is borne by the operator.

The certification shall be subject to an annual update.

A decree shall determine the conditions for the application of this III.'

Article 34 of Law No 2010-476 of 12 May 2010 on the opening-up to competition and regulation of the online gambling and games of chance sector:

'VIII. — The National Gaming Authority determines the technical characteristics of online gaming and betting platforms and software for operators subject to a licensing regime and operators with exclusive rights. It periodically assesses the level of security. […]

It determines the technical requirements for the integrity of gaming operations and the security of information systems with which operators must comply. It determines the technical parameters of online games for the application of the decrees provided for in Articles 13 and 14 of this Law.

It shall ensure the quality of the certifications carried out in accordance with Article 23. It shall draw up the list of certifying bodies and may amend it. It is the recipient of the certification reports provided for in the same article.

It assesses the internal controls put in place by operators. To this end, it may conduct or request any audit of information systems or processes.

Under the conditions set by decree, it shall assess the results of the actions taken by the operators in terms of the integrity of the game and the information system and can make regulations for them on this matter. […]'

Provisions of Articles 11 to 24 of Decree No 2020-1349 of 4 November 2020 on the rules for regulating the National Gaming Authority:

'Chapter 1: Conditions for inclusion in the list of certifying bodies (Articles 11 to 15)[...]

Chapter 2: Obligations of certifying bodies (Articles 16 to 19) [...]

Chapter 3: Certification duties (Articles 20 to 24)

Article 20:

In accordance with the provisions of Article 23 of the above-mentioned Law of 12 May 2010, the certification process shall concern the operator's compliance with all the technical requirements applicable to their activity.

The National Gaming Authority shall determine the method, nature and extent of the inspections performed by the certification body.

Article 21:

The analysis operations carried out by the certifying body shall not be iterative during the same certification: each controlled requirement is subject to a single check. Exchanges may take place at the time of the inspection between the certifying body and the operator whose certification it is checking. However, once the check has been carried out, such exchanges may not under any circumstances lead the certifying body to carry out a new analysis.

In particular, changes, if any made by an operator in the course of certification at a control point already measured, cannot alter the initial finding which must be included in the certification report.

Article 22:

At the end of its work, the certification body shall write up a report setting out its findings. This report shall list all the non-conformities found, regardless of their severity.

The report concludes either a certification without reservation, or a certification with reservations. Certification shall be made with reservations where one or more technical requirements with a critical level defined by the technical reference are not met.

The certification body shall send the operator the document certifying that it has obtained the certification referred to in Article 23 of the above-mentioned Law of 12 May 2010 so that they may

proceed with the submission provided for in this Article. This document shall indicate whether the certification is obtained with or without reservation and shall indicate, where applicable, the reservation(s) concerned.

Article 23:

Once the certification report has been submitted, the operator shall, if applicable, write up vulnerability records and send them to the National Gaming Authority within one month of submission of the report. These vulnerability records are sent, for information purposes, to the certification body.

The vulnerability records are separate from the certification report. They shall include a list of all the non-conformities found in the certification report, regardless of its severity. For each point of non'compliance, the operator shall, where necessary, propose corrective measures and an implementation schedule.

These vulnerability records may also enable the operator to inform the National Gaming Authority of any relevant information or observations concerning the conduct of the certification operations and/or to inform it of any disagreement with the conclusions of that report or with the methodology used. The operator may, if necessary, carry out a new check and produce the result by transmitting the vulnerability records to the National Gaming Authority.

Article 24:

The bodies registered on the list of certification bodies, because of their technical expertise prior to the date of publication of this decree, will remain on the list until the end of the term set by the provisions in force on the date of their registration.

The bodies registered on the list of certification bodies, because of their technical expertise as subcontractors prior to the date of publication of this decree, will remain on the list until the end of the term set by the provisions in force on the date of their registration. They may propose certification missions primarily under the provisions of this decree, as of its publication.'

Article L.231-1 of the Code of Relations between the Public and the Administration:

'Silence on the part of the administration for two months regarding a request constitutes acceptance.'

Article 1 of Decree No 2015-397 of 7 April 2015 on the system of decisions regarding registration on the list of bodies for certification and approval of gaming or betting software taken by the Authority for the regulation of online gambling:

'Under Article L231-4(4) of the Code of Relations between the Public and the Administration, the decision to reject:

1. Silence for two months on the part of the National Gaming Authority regarding an application for registration on the list mentioned in Article 23(II) of the above-mentioned law of 12 May 2010;

2. Silence for two months on the part of the National Gaming Authority regarding an application for approval of gaming or betting software made by an online gaming or betting operator under Article 34(III)(2)[1] of the above-mentioned Law of 12 May 2010.'

I.2 Presentation of the document and the objectives of the certification

The provisions of Article 23 of Law No 2010-476 of 12 May 2010 on the opening up to competition and the regulation of the online gambling sector, as amended by Order No 2019-1015 of 2 October 2019 reforming the regulation on gambling, subject authorised online gambling operators and operators with exclusive rights to a certification procedure.

This must be carried out by an independent body chosen by the operator from a list drawn up and updated by the National Gaming Authority, the drawing up and updating of which constitutes one of the levers enabling the Authority to ensure the quality of the certifications in accordance with the provisions of VIII of Article 34 of this law.

The objective of this certification is to ensure that the operators comply with all the technical requirements applicable to their activity, in particular those determined by the Authority concerning the integrity and reliability of gaming operations and the security of information systems, that implement the objective of the State's gambling policy set out in point 2 of Article L.320-3 of the Internal Security Code.

The activities carried out by the Authority in this context are, more broadly, part of the control system it has put in place to meet all the objectives set out in Article L.320-3 of that Code.

In this context, the purpose of this document is to set out:

- the conditions for the listing and de-listing of the certifying bodies resulting from the provisions of Chapter 1 of Title III of Decree No 2020-1349 of 4 November 2020 on the rules governing the regulation of the National Gaming Authority;
- the obligations applicable to certifying bodies included in the National Gaming Authority list, as set out in Chapter 2 of Title III of Decree No 2020-1349 of 4 November 2020 referred to above;
- the detailed rules for the implementation of the certification duty, as resulting in particular from the provisions of Chapter 3 of Title III of Decree No 2020-1349 of 4 November 2020 referred to above, and which are intended in particular to recall:
  - the area of the certification, i.e. the cases in which the certification is to be conducted;
  - the scope of the certification, i.e. all the elements to be covered by the different certification audits;
  - deliverables expected.

[1] This is in practice the second paragraph of Section VIII, following a renumbering of the articles, inaccurately referenced here.

I.3 Glossary

ANJ: National Gaming Authority [Autorité Nationale des Jeux].

Authenticity: the nature of information (document, data) which can be proven to be genuine, to have been effectively produced or received by the person claiming to have produced or received it, and to have been produced or received at the time stated.

Sensor: a component of the physical storage medium (i.e. PSM (in French SMA)), whose function is to create traces. The trace creation function corresponds to the formatting of the data circulating between the player and the game platform and the transfer of that data to the vault module of the physical storage medium (PSM).

Certification: an analysis operation which allows a client to ensure, through the intervention of a verified and competent independent professional, referred to as a certifying body, the compliance of a product with a standard.

Vault: a component of the physical storage medium (PSM (in French SMA)), whose function is to encrypt, sign, time stamp and archive the data traced and collected from the stream from the player or provided by the game platform. This is in order to guarantee confidentiality, authenticity and completeness over time.

Confidentiality: the property that the information is not made available or disclosed to unauthorised persons, entities or processes.

Integrity: the complete and unaltered nature of information proving that it has not undergone any addition, withdrawal or accidental or intentional modification, since its validation.

Gaming platform: all the technical infrastructure implemented for the purpose of providing gambling services to players or betters. Infrastructure or service elements can be managed on their own by the operator or by third parties (examples: hosting by a third party, third-party infrastructure, gaming software solution provided by a third party).

Information system (IS): Structured set of technical resources (computer hardware, network equipment, software, business processes and procedures) and social resources (organisational structure and IS-related people) within an organisation, designed to develop, collect, process, classify, store, and disseminate information.

Physical Storage Medium (PSM (in French SMA)) – système matériel d'archivage (SMA): a device for collecting and storing data exchanged between the player and the operator's gaming platform during gaming operations. This device shall be developed and operated under the responsibility of the operator. It consists of the 'sensor' and 'vault' components.

Traceability: a property that allows non-repudiation and ensures accountability. This means that this property guarantees the origin of the source, the destination, the veracity of an action and the identification of the entity responsible.

I.4 Identification of requirements and recommendations in the document

This document has two levels of measures:

- The measures preceded by **[E_numero]** are requirements that are **obligatory**, subject to the exceptions mentioned in these technical requirements;
- The measures preceded by **[R_numero]** are recommendations, which operators may decide not to follow, subject to justification to the Authority and reporting to the Authority the alternative measures they intend to implement.

II ‘Certifiers’ part

II.1 Procedures regarding the list of certifying bodies

Certifying bodies shall be subject to the following procedures:

a) Initial enrolment on the list of certifying bodiesby which the Authority, after examination of the application file, habilitates the certifying body to conduct certifications for gaming operators;
b) Renewal enrolment on the list of certifying bodiesat the end of a period of 5 years which results in a new habilitation of the certifying body after examination by the Authority of a new file containing the same updated documents as those requested in the file for the initial listing;
c) Withdrawal from the list of certifying bodies: the request for withdrawal – before the expiry of the 5-year period of validity of the listing – must be notified by the certifier to the Authority by registered mail in order to allow the list of certifying bodies listed for operators to be kept up-to-date. Conversely, the ANJ may proceed to the withdrawal from the list a certifying body, by a motived decision.

The corresponding procedures and deliverables are detailed below.

II.1.1 Procedure for initial enrolment and renewal after 5 years

The enrolment corresponds to the inclusion on the list of certifying bodies.

[E_CRT_REF1] In accordance with the provisions of Article 12 of Decree No 2020-1349, the list of certifying bodies may include only bodies who:

- are established in a European Union Member State or a State party to the Agreement on the European Economic Area;
- have sufficient skills and appropriately qualified staff;
- carry out their certification tasks independently and impartially.

[E_CRT_REF2] The application file for initial listing is submitted to the ANJ in accordance with the procedures laid down in Article 13 of Decree No 2020-1349 of 4 November 2020. This folder, transmitted in a dematerialised format, includes the following:

1. The enrolment application form;
2. A document showing the references of services performed by the applicant in areas of expertise similar to those required to issue the certification (see requirement [E_CRT_LRA1], section II.2);
3. The list of persons dedicated to certification operations and their detailed curriculum vitae (see requirement [E_CRT_LRA2], section II.2);
4. Standard analysis reports highlighting the methodologies used and the scope of analyses conducted in the field of intrusive application audits and hosting platform configuration audits.

[E_CRT_REF3] The enrolment renewal application file submitted by an accredited certification body to the ANJ in a dematerialised format shall include the same updated documents as those transmitted in the case of initial enrolment (see requirement [E_CRT_REF2]).

[E_CRT_REF4] Should the application file be incomplete, a letter shall be sent to the applicant inviting the applicant to forward, within a period not less than 15 days, the missing document(s). Examination of the registration application shall be suspended during this period.

Any application which is still incomplete at the end of the prescribed period shall result in the ANJ issuing a decision rejecting the enrolment or its renewal.

[E_CRT_REF5] During the course of the investigation, , if requested by the Authority to clarify its file, the applicant is required to provide additional information. In addition, the applicant may be interviewed by the ANJ.

[E_CRT_REF6] The decision of the Authority is notified to the applicant within two months from the reception of the application file. The certifying body shall then receive a reference number of his initial or renewed enrolment and be included in the list of certifying bodies.

II.1.2 Withdrawal procedure

[E_CRT_PRS1] A certifying body enrolled on the list of vertifiying bodies may request its withdrawal from the list before the expiry of the 5-year period of validity of the listing, by notifying the Authority of its withdrawal request by registered mail.

Within at most two months from the reception of the withdrawal request, the certifying body shall be removed from the list of certifying bodies.

[E_CRT_PRS2] In accordance with the provisions of Article 19 of Decree No 2020-1349 of 4 November 2020, if a certifying body no longer possesses the qualifications required to be included in the list of certifying bodies, the ANJ may, by motivated decision, proceed to its withdrawalfrom the list of certifying bodies. In such a case, before proceeding to the actual withdrawal, the Authority notifies by mail its intention to the certifying body which has 15 calendar days to submit its observations and explanations by mail.

II.2 Specifications of expected deliverables

[E_CRT_LRA1] The document showing the references of services performed by the applicant in areas of expertise similar to those required to issue the certification shall specify for each reference:

1. the precise scope of the service;
2. its duration
3. the customer;
4. the period during which the auditswere carried out;
5. the names and surnames of the auditors who carried out the task.

[E_CRT_LRA2] The list of individuals dedicated to certification operations and their detailed curriculum vitae will include:

1. the names and surnames of these persons;

2. a synthetic description of the certification missions carried out by these persons;
3. their seniority within the certifying body staff and the function(s) they have held.

II.3 Obligations of certifying bodies

Certification duties are the responsibility of the certifying officers in accordance with the requirement [E_CRT_AUD1]. In carrying out these duties, the certifying officers are subject to a number of obligations described below.

[E_CRT_OOC1] The body inscribed on the list of certifying bodies shall carry out the certification mission in accordance with the state of the art.

[E_CRT_OOC2] In accordance with the provisions of Article 17 of Decree No 2020-1349 of 4 November 20220, the certifying body is independent from the operator for whom it carries out the certification mission.

In particular, it may not carry out any certification assignment for a gaming operator if it has been its consultant or provider, or that of any company controlling[2] the gaming operator, within the 12 months preceding the signature of the certification contract with the operator.

[E_CRT_OOC3] The organisation on the list of certifying bodies shall inform the ANJ without delay of any situation of conflict of interest arising in relation to its certification activity.

[E_CRT_OOC4] A copy of the certification contract between the certifying body and the certified operator shall be communicated to the Authority by the operator upon completion of the certification service.

[E_CRT_OOC5] The body on the list of certifying bodies shall inform the ANJ without delay of any changes to the list of persons in charge of certification operations. The curriculum vitae of any new person incorporated into this list must then be submitted to the ANJ.

[2] within the meaning of the Commercial Code

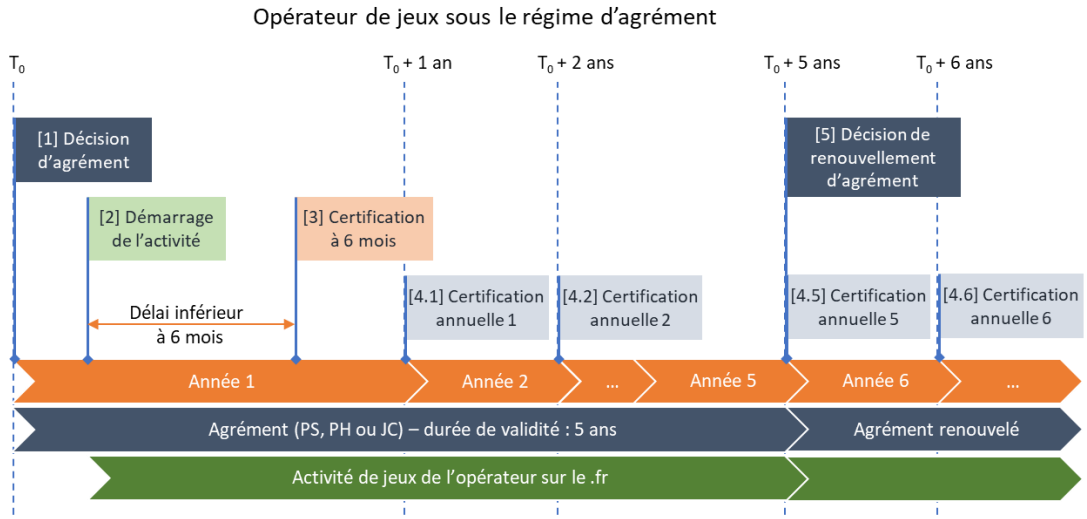
III ‘Certification’ part

III.1 Scope

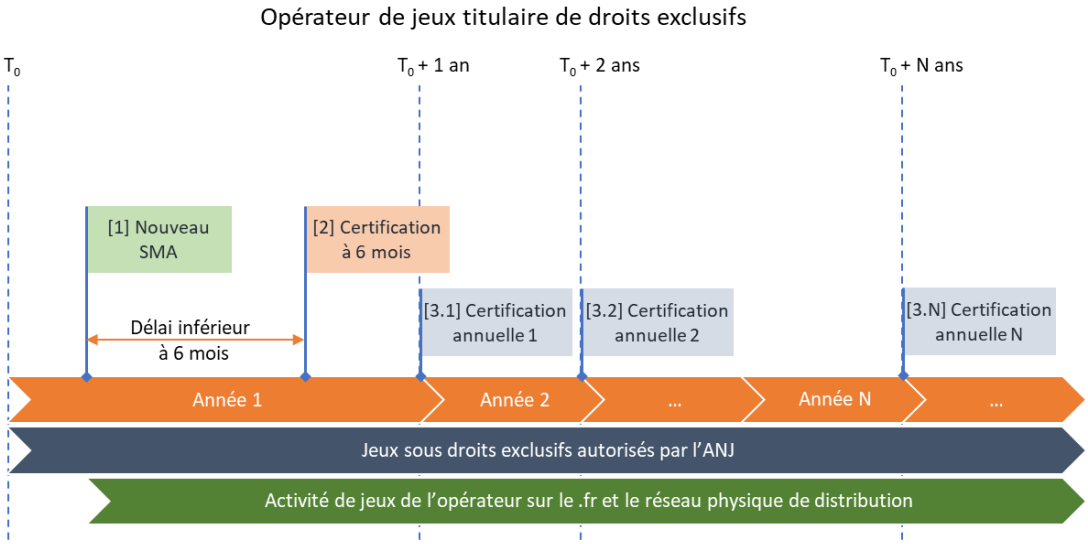
[E_CRT_CHA1] Certification is a procedure that applies, on the one hand, to licensed gaming operators holding one or more licences issued by the Authority pursuant to Article 21 of Law No 2010-476 of 12 May 2010, referred to in this document as ‘licensed operators’, and, on the other hand, to operators also holding exclusive rights.

It consists of two sub-procedures:

a) A 6-month certification to be conducted before the 6-month deadline following the start of operation of a new PSM (In French SMA);
b) An annual certification to be carried out annually (i) on the anniversary date of obtaining authorisation for authorised operators or (ii) on a date fixed by the ANJ jointly with the operator, for operators with exclusive rights (cf requirement [E_CRT_PER3]).



Opérateur de jeux sous le régime d’agrément	Gaming operators under the license scheme
1 an	1 year
[1] Décision d’agrément	[1] Approval decision
[2] Démarrage de l’activité	[2] Start of the activity
Délai inférieur à 6 mois	Time limit less than 6 months
[3] Certification à 6 mois	[3] 6-month certification
[4.1] Certification annuelle 1	[4.1] Annual certification 1
[5] Décision de renouvellement d’agrément	[5] Decision to renew the license
Année	Year
Agrément (PS, PH ou JC) – durée de validité : 5 ans	License (PS, PH or JC) – period of validity: 5 years
Agrément renouvelé	Renewed license
Activité de jeux de l’opérateur sur .fr	Operator’s game activity on .fr



Opérateur de jeux titulaire de droits exclusifs	Gaming operator with exclusive rights
1 an	1 year
[1] Nouveau SMA	[1] New PSM (in French SMA)
[2] Certification à 6 mois	[2] 6-month certification
Délai inférieur à 6 mois	Time limit less than 6 months
[3.1] Certification annuelle 1	[3.1] Annual certification 1
Année	Year
Jeux sous droits exclusifs autorisés par l'ANJ	Exclusive rights games authorised by the ANJ
Activité de jeux de l'opérateur sur le .fr et le réseau physique de distribution	Operator's gaming activity on .fr and physical distribution network

[E_CRT_CHA2] If the operator has multiple approvals, a single annual certification is carried out.

[E_CRT_CHA3] The certifying body's report and its conclusion on the 6-month or annual certification obtained — with or without reservations — must be submitted to the ANJ as scheduled (cf. sections III.3.2 et III.3.3).

Certification does not give rise to the notification of a decision by the Authority. It may however, in the case of significant reservations and depending on their gravity, lead to an enquiry by the Authority based on article 42 of law No 2010-476 of 10 May 2010 as amended. The enquiry may itself conduct the Authority to place the matter before the sanction commission in application of article 43 of the same law.

III.2 Perimeter covered by certification

III.2.1 6-month certification

[E_CRT_PER1] Provided in Article 23 II of Law No 2010-476 of 12 May 2010, the single 6-month certification relates to the PSM (in French SMA) and its hosting infrastructure.

III.2.2 Annual certification

[E_CRT_PER2] As set in in Article 23 III of Law No 2010-476 of 12 May 2010, the annual certification perimeter covers the information system providing the gaming and betting services delivered by the operator, including the gaming plateform of subcontractors as the case may be, as well as changes to approved softwares since it was last approved. This scope also includes the PSM (in French SMA) with respect to security matters and, where appropriate, its techno-functional aspects if it has undergonesubstantial evolutions.

What is a substantial evolution of the PSM (in French SMA)?

A development shall be classified as substantial when either:

1. It calls into question the functioning of the PSM (in French SMA);
2. It calls into question the PSMs's security analysis.

The functioning of the PSM may be called into question when the development relates to one or more of the following:

3. A change in the strategy for the creation and collection of traces;
4. A change in the strategy for the archiving of traces;
5. A change in the strategy for accessing and extracting traces.

The safety analysis may be called into question when the development relates to one or more of the following:

6. A development modifying all or part ofthe mechanisms or configurations directly impacting the security of the PSM (examples: authentication, access control, communications encryption);
7. A development modifying the internal architecture of the PSM;
8. A development corresponding to the replacement of a technology by another within the PSM (examples: framework, software library, programming language), excluding version upgrade;
9. A modification of infrastructure modifying the exposure in terms of IT security of the PSM (examples: change of hosting site, gaming platform provider or vault provider);
10. The addition or modification of one or more direct interconnections to the PSM with other information systems.

The ANJ does not consider the following to be substantial developments, provided that the changes made do not fall under one of the above two cases (i.e. points 1 and 2):

11. The upgrading of the version of the PSM or any of its components;
12. The fixing of bugs and potential vulnerabilities;
13. Modifications of the graphic chart or the ergonomy of the user interface of the PSM

The National Gaming Authority reserves the right to revise the qualification of the development adopted by the operator on the basis of the conclusions of the previous certification work and the controls carried out by the ANJ.

[E_CRT_PER3] For operators with exclusive rights, on part of the information system providing for the games under exclusive rights, and for that part only, the certification may be covered by annual sector certification, providing overall coverage over a multi-year cycle of 2, 3, 4 or 5 years, with the exception of (i) the security of the PSM (in French SMA), (ii) external[3] intrusion testing of the gaming platform and (iii) control of remediation plans, which remain under anannual certification control.

A sector shall be understood as a coherent technical-functional scope of the operator's information system, providing services for the games under exclusive rights, including the services of third-party suppliers where appropriate.

The duration of the cycle and certification programme and timetable for each of the years of the cycle, which must cover the entire scope subject to certification throughout the cycle, shall be the subject of a formal written proposal to the Authority by the operator with exclusive rights, submitted no later than 6 months before entry into a new cycle.. The certification programme for each of the years of the cycle may be based on the sectors defined in a dedicated annex.

The Authority shall validate, within two months of the submission of the proposal, the proposed programme, and may request modifications. The decision establishing the certification programme remains the Authority prerogative.

In the absence of a formalised written proposal by the operator with exclusive rights at the latest 6 months before entering a new cycle, the certification will be deemed to follow an annual pace, with a scope covering all sectors subject to certification.

Regarding approved softwares, in the context of a multi-year certification, the scope of the check will be restricted to those belonging to the sectors to be covered by the certification in the current year, unless requested otherwise by the Authority in the notification letters accompanying the homologation decisions taken at the lastest one month before the submission of the certification file.

[3] Internal intrusion tests will be performed by sector, according to the agreed certification program.

III.3 Certification procedures

III.3.1 Provisions common to certification tasks

III.3.1.1 Performance of certification audits

[E_CRT_AUD1] The certification — after 6 months or annually — is carried out by an independent body chosen by the operator from the list of certifying bodies drawn up by the ANJ. The cost of this certification shall be borne by the operator.

[E_CRT_AUD2] Audit operations carried out by the certifying body are carried out on the basis of the technical reference framework, established by the technical requirements set down in this document and its annexes (in particular, the 6-month certification requirement matrix and the annual certification requirement matrix).

Compliance and safety requirements shall be subject to several checkpoints, which are presented in the technical reference framework.

[E_CRT_AUD3] For each technical reference inspection point, the certifying body shall complete the relevant requirements matrix (see Annex 2), indicating the compliance of the assessed requirement and its criticality level (see Annex 3) resulting from its analysis. This assessment must take into account the information provided by the operator (examples: documentation resources, source codes), tests and technical audits carried out by the certifying body, as well as certificates of absence of modification provided, where appropriate, by the operator.

[E_CRT_AUD4] Analysis operations conducted by the certifying body are not iterative during a givencertification rollout: each controlled requirement is subject to a single check.

Exchanges may take place at the time of the check between the certifying body and the operator whose certification it is checking. However, once the check has been carried out, such exchanges may not under any circumstances lead the certifying body to carry out a new analysis. In particular, changes, if any, made by an operator in the course of certification at a control point already measured cannot alter the initial finding which must be included in the certification report.

[E_CRT_AUD5] At the end of the certification task, the certifying body shall establish:

1. The certification report showing the findings made (see III.4.1 and III.4.2);
2. The certificate of certification.

The report shall list all the non-conformities found, regardless of their severity. The report concludes either a certification without reservation, or a certification with reservations, which must be explicitly mentioned.

Certification is granted with reservations when one or more technical requirements whose severity is greater than or equal to 2 are not met or when vulnerabilities of significant, major or critical severity have been identified.

The certification certificate shall reflect only the nature of the certification with or without reservations andindicate the existing reservation(s) if there are any.

[E_CRT_AUD6] The certification report and certificate shall be signed electronically by the certifying body which is the author of the certification report, in accordance with the standard set out in Annex 5 to this document. The electronic signature files obtained accompany the certification report and the certificate respectively.

In order to verify the authenticity of the signed documents, the certifying body shall communicate to the ANJ, upon completion of the certification service, its public key *via* the means of exchange made available by the ANJ.

[E_CRT_AUD7] At the end of the certification task, the certifying body shall transmit to the operator concerned the electronically signed report and certificate of certification so that the operator sends them to the ANJ for the 6-month certification (see III.3.2) and the annual certification (see III.3.3).

III.3.1.2 Non-conformities and vulnerabilities

[E_CRT_CAN1] Any non-conformity identified during the certification work shall be subject to a remediation plan. They must be corrected within a period not exceeding twelve months from the date of submission of the remediation plan or, should the operator fail to submit it within the time frame set by requirements **[E_CRT_ASM2]** et **[E_CRT_ANN2]**, from the end of submission time frame defined by these requirements. The corrections made must be validated by the certifying body as part of the next annual certification.**[E_CRT_CAN2]** Any vulnerability identified during certification work, in particularl during intrusion tests, must be subject to a remediation plan. They must be corrected within a period not exceeding three months for major or critical vulnerabilities[4], six months for significant vulnerabilities and twelve months for minor vulnerabilities, from the date of submission of the remediation plan or, should the operator fail to submit it within the time frame set by requirements **[E_CRT_ASM2]** et **[E_CRT_ANN2]**, from the end of submission time frame defined by these requirements. The corrections made must be validated by the certifying body as part of the next annual certification.

[E_CRT_CAN3] If security measures do not directly correct vulnerabilities, the operator will have to propose compensatory measures to avoid their beingexploited and present them in the remediation plan. Compensatory or perimeter protection measures shall be validated by the certifying body within the framework of the next annual certification.

[E_CRT_CAN4] The operator shall justify in the remediation plan any refusal to correct the vulnerabilities and non-conformities identified during the certification work and, where appropriate, present the alternative measures it proposes. The assessment of the merits of the justifications and, where appropriate, alternative measures presented by the operator shall be the responsibility of the ANJ.

[R_CRT_CAN5] In order to lift a reservation (including major or critical vulnerabilities and level 3 non-conformities), the operator may, if necessary, have the certifying body re-check and produce the result with the transmission of vulnerability records to the ANJ.

[4] Refer to the vulnerability severity scale defined in Annex 4 to this document.

III.3.1.3 Remediation plan

[E_CRT_PRM1] The operator shall draw up a remediation plan, which shall contain, for each vulnerability or non-conformity identified in the certification report, a record containing at least three components:

1. A summary description of the vulnerability or non-conformity. In the case of a vulnerability, the associated risk level (see Annex 4) must also appear on the record;
2. The certifying body's recommendations to correct the v or non-conformity;
3. The remediation plan justifying the operator's management of the vulnerability or non-conformity. The remediation plan details the actions taken or planned by the operator to correct the vulnerability or non-conformity (including compensatory measures) and specifies the planning for these actions.

[E_CRT_PRM2] For critical, major or significant vulnerabilities and non-conformities with critical level equal or above 2, the operator is required to report to the ANJ on the completion of the remediation plan according to the communicated planning A grouping of reports by quarter is possible.

III.3.2 Deadline for submission of 6-month certification documents

[E_CRT_ASM1] Within six months from the date of entry into operation of the PSM (in French SMA), the licenced operator or holder of exclusive rights shall transmit to the ANJ:

1. The electronically signed certification report ;
2. The electronically signed certificate of certification.

[E_CRT_ASM2] The remediation plan shall be sent by the operator to the ANJ and the certifying body within one month of the submission of the certification report.

III.3.3 Deadline for submission of annual certification documents

[E_CRT_ANN1] Within one year from the date of obtaining the license, or the date established for operators with exclusive rights, the gaming or betting operator shall transmit to the ANJ:

1. The electronically signed certification report ;
2. The electronically signed certificate of certification.

[E_CRT_ANN2] The remediation plan shall be sent by the operator to the ANJ and the certifying body within one month of the submission of the certification report. If the operator changes the certifier the following year, they will also have to forward the remediation plan to the new certifying officer prior to the latter's work.

[E_CRT_ANN3] The certification shall be updated annually by no later than the anniversary date of the previous certification.

III.4 Deliverables

III.4.1 Deliverables for 6-month certification

The checks carried out during the 6-month certification, covering the PSM (in French SMA), are based on a basis of mandatory analyses, as described below.

III.4.1.1 Deliverables expected

[E_CRT_LCA1] 6-month certification deliverables should be delivered to the ANJ in a dematerialised format.

[E_CRT_LCA2] The 6-month certification deliverables are as follows:

1. The certification report produced by the certifying body, electronically signed in accordance with requirement [E_CRT_AUD6] (see section III.3.1.1);
2. The certificate of certification produced by the certifying body, electronically signed in accordance with the requirement [E_CRT_AUD6] (see section III.3.1.1);
3. The remediation plan for non-conformity and vulnerabilities identified during certification audits, produced by the gaming or betting operator.

III.4.1.2 Content of the certification report

[E_CRT_LCA3] The 6-month certification report shall consist, for each approval or scope of activity, of the following 6 documents:

1. A summary of the reports mentioned in points 3, 4 and 5, including reservations if any;
2. The duly documented requirements matrix;
3. The functional, technical and security audit report of the sensor;
4. The PSM (in French SMA) configuration audit report (i.e. sensor and vault) and its hosting infrastructure;
5. The report verifying compliance with requirements;
6. The technical annexes.

[E_CRT_LCA4] The summary of reports will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. The presentation of the applicant operator;
2. A reminder of the name and contact details of the certifying body responsible for carrying out the certification;
3. The dates of the various audit services;
4. The workload (in man-days) devoted to each checkpoint;
5. The date of the operational implementation of the PSM (in French SMA);
6. The strategic summary of results obtained by control point;
7. A list of all identified vulnerabilities and non-conformities.
8. The exhaustive and detailed list of reservations.

[E_CRT_LCA5] The functional, technical and security audit report of the sensor will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. Summary of the audit:
    a. Summary of the functional and technical audit;
    b. Summary of the intrusive audit (code audit and intrusion tests);
    c. Summary of non-conformities, classified by severity and impact;
    d. Summary of vulnerabilities, classified by severity and impact;
    e. Summary of recommendations, classified by severity and cost of implementation;
2. Functional and technical audit of the sensor:
    a. Presentation of the solution and compliance of implementation:
        i. Trace creation and recording mechanisms;
        ii. Data verification and filtering mechanisms;
        iii. Sensor security mechanisms;
    b. Source code audit of sensor functionalities;
3. Intrusive sensor audit:
    a. Linear conduct of intrusive sensor audit, with an explicit description of the methodology used to detect and exploit vulnerabilities, where appropriate;
    b. Source code audit of sensor security.

As part of the functional and technical audit of the sensor, the certifying body does not perform syntactic and semantic analysis of recorded traces in XML format but shall ensure that the implementation of the sensor complies with the technical requirements for data made available to the ANJ (ET3) and that all records produced by the sensor are properly formatted according to the XML standard and XSD schemas published by the ANJ.

In the context of the intrusive sensor audit, the certifying body is expected to try, through intrusion tests, for example by injecting specially forged traces into the vault in order to divert its recording and security functions (examples: corruption of records, injection of false events), (i) to get remote control of the sensor and vault, and (ii) to manipulate of betting or account management records.

[E_CRT_LCA6] The configuration audit report of the PSM (in French SMA) and its hosting infrastructure will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. Summary of the audit:
    a. Technical summary of the configuration audit;
    b. Summary of vulnerabilities, classified by severity and impact;
    c. Summary of recommendations, ranked by priority and cost of implementation;
2. Configuration audit:
    a. Analysis of the security strategy (technical security policy, procedures, etc.) ;
    b. Analysis of the technical architecture (flow matrices, firewall rules, etc.) ;
    c. Analysis of configurations at system, network and application levels.

[E_CRT_LCA7] The compliance verification report brings together the various analyses (and their results) that have not been addressed in previous deliverables.

III.4.1.3 Content of the technical annexes

[E_CRT_LCA8] The technical annexes consist of the operator's documentation relating to the PSM (in French SMA) (sensor and vault), including details of the solution implemented.

III.4.2 Deliverables for annual certification

III.4.2.1 Updateability of the annual certification deliverables

Annual certification is based on a set of analyses that may or may not be partially or totally updated, *via* differential audits. This is referred to as an updateable analysis.

Updating refers to the repeat in part or in full of checks carried out during an earlier certification on a given perimeter.. In such a case, the deliverables are only expected to be updated with the new results obtained and the associated comments.

A certificate of absence of modification produced by the operator may also lead the certifying body not to carry out an analysis on the concerned perimeter, provided that this lack of modification does not deter the security maintenance of the information system covered by the certification.

[E_CRT_LCB1] Not all analyses can be dealt with a mere updating nor avoided by an operator's certificate of absence of modification. In particular:

1. The points of verification which would have been subject to reservations in the previous certification must be subject to a new analysis;
2. Intrusion tests, internal [5] and external, must be performed in full each year.

The updatable analyses are identified in green color in this section. The requirement [E_CRT_LCB13] specifies the conditions for performing differential audits.

III.4.2.2 Deliverables expected

[E_CRT_LCB2] The annual certification deliverables are as follows:

1. The certification report produced by the certifying body electronically signed in accordance with the requirement [E_CRT_AUD6] (see section III.3.1.1);
2. The certification certificate produced by the certifying body electronically signed in accordance with the requirement [E_CRT_AUD6] (see section III.3.1.1);
3. The remediation plan for non-conformities and vulnerabilities identified during certification audits, produced by the gaming or betting operator.

[E_CRT_LCB3] The annual certification deliverables are to be delivered to the National Gaming Authority in a dematerialised format.

[5] Except in accordance with the requirement [E_CRT_PER3] where only external intrusion tests are to be performed annually on the entire scope subject to certification.

III.4.2.3 Content of the certification report

[E_CRT_LCB4] The annual certification report shall consist, for each approval or scope of activity, of the following documents:

1. A summary of the reports mentioned in points 3 to 8 including any reservations;
2. The duly documented requirements matrix;
3. The report of the internal and external intrusion tests of the gaming platform, including the PSM (in French SMA) sensor component;
4. The functional and technical audit report of the sensor;
5. The audit report of the technical architecture of the gaming platform;
6. The gaming platform equipment configuration audit report;
7. The audit report on developments in gaming software;
8. The report verifying compliance with requirements;
9. The technical annexes.

[E_CRT_LCB5] The summary of reports will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. The presentation of the applicant operator;
2. A reminder of the name and contact details of the certifying body in charge of the certification;
3. The dates when the various audits were conducted;
4. The workload (in man-days) devoted to each checkpoint;
5. The date of the operational implementation of PSM (in French SMA) developments where applicable;
6. The strategic summary of results obtained by control point;
7. A list of all identified vulnerabilities and non-conformities.
8. The exhaustive and detailed list of reservations;

[E_CRT_LCB6] The report of the internal and external intrusion tests of the gaming platform, including the PSM (in French SMA) sensor component, will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. Summary of the audit:
    a. Summary of intrusion tests;
    b. Summary of vulnerabilities, classified by severity and impact;
    c. Summary of recommendations, classified by severity and cost of implementation;
2. Intrusion tests:
    a. A synthetic technical risk analysis;
    b. Linear conduct of the audit of internal and external intrusion tests of the gaming platform including the sensor, with an explicit description of the methodology used to detect and exploit vulnerabilities, if any.

[E_CRT_LCB7] The functional and technical audit report of the sensor will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. Summary of the audit:
    a. Summary of the functional and technical audit;
    b. Summary of non-conformities, classified by severity and impact;

c. Summary of recommendations, ranked by priority and cost of implementation;

2. Functional and technical audit of the sensor:
    a. Presentation of the solution:
        i. Trace recording mechanisms;
        ii. Data verification and filtering mechanisms;
        iii. Sensor security mechanisms;
    b. Audit of the source code for the most important functions of the sensor.

[E_CRT_LCB8] The technical architecture audit report of the gaming platform will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. Summary of the audit:
    a. Technical summary of the architecture audit;
    b. Summary of vulnerabilities, classified by severity and impact;
    c. Summary of recommendations, classified by severity and cost of implementation;
2. Architecture audit:
    a. Presentation of the technical architecture;
    b. Analysis of the technical architecture (network diagram (level 3), flow matrices, filtering rules, etc.) ;
    c. Partitioning analysis;
    d. Administrative mechanisms.

[E_CRT_LCB9] The gaming platform equipment configuration audit report will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. Summary of the audit:
    a. Technical summary of the equipment audit;
    b. Summary of vulnerabilities, classified by severity and impact;
    c. Summary of recommendations, ranked by priority and complexity of implementation;
2. Configuration audit: analysis of configurations at system, network and application levels.

As part of the configuration audit, the certifying body may sample the components to be audited by role and/or criticality. In subsequent certifications, the knowledge base built on the basis of the analyses should allow the certifying body to review its sampling and refocus its audit on components that would not have been thoroughly analysed in previous certification. However, system security controls must be carried out systematically (i.e. status of updates, user account management, rights management, password complexity, time synchronisation, etc.).

[E_CRT_LCB10] The audit report on the evolutions of different gaming software will follow the detailed plan below. It may contain additional sections if the operator or certifying body deems it necessary:

1. Summary of the audit;
2. Audit of gaming software developments:
    a. List of different gaming software used (clients and server);
    b. Analysis of changes made.
    c. Monitoring the effective implementation of the remediation plans for approved games in accordance with the timetables of those plans. The certifying officer will refer to the technical requirements for approvals, sections IV.1.2 and IV.1.3, as regards the agreed maximum time limits for correction.

[E_CRT_LCB11] The compliance verification report brings together the various analyses (and their results) that have not been addressed in previous deliverables.

III.4.2.4 Content of the technical annexes

[E_CRT_LCB12] The technical annexes consist of the following documents:

1. Operator's documentation;
2. The operator's attestations of the lack of modification of the elements referred to in the technical and functional audits required above, where applicable.

III.4.2.5 Special provisions

[E_CRT_LCB13] As part of the annual certification, technical and functional audits may be conducted in a differential manner, covering only those components that have evolved since the previous certification, without re-examining the unaltered components. Where applicable, the unaltered components shall be subject to a specific attestation of the lack of modification referred to in point 2 of the requirement [E_CRT_LCB12]. For unaltered components, the corresponding requirement matrix should then replicate the results obtained during the previous certification.

This possibility of differential audit of functional and technical audits, aimed at simplifying and reducing certification, does not apply to security audits which must be carried out each year.

[E_CRT_LCB14] The possibility is offered to the operator, for the purpose of reducing the annual certification, to use the audit reports carried out under ISO certifications of the World Lottery Association (WLA) or equivalent, provided that the following constraints are met:

1. ISO, WLA, or equivalent audits shall not be older than 9 months from the date of submission of the certification report to the National Gaming Authority;
2. ISO, WLA, or equivalent certification reports do not replace the annual certification report. Deliverables requested by the Authority (e.g. audit reports, specified requirement matrix, certification certificate) are still produced by the certifying body, but their audit sections may display a precise reference to one or more sections and pages of the ISO, WLA or equivalent audit report(s) covering the control point or appropriate requirement;
3. The certifying body shall ensure that all the requirements of the annual certification are covered.

For operators with exclusive rights, the activation of this proposed option to use such reports will have to be declined in the context of requirement [E_CRT_PER3] and will be explicitly included in the multiannual programme submitted to the Authority.

IV Annexes

IV.1 Annex 1 – Types of audit services expected

IV.1.1 Intrusion test

The objective of an intrusion test service is to search for and exploit vulnerabilities discovered on a system. This is not just an automated vulnerability test. Detailed manual tests should also be included in the report.

The analysis must reveal the different classical stages of the intrusion test (printing, vulnerability search, manual tests, etc.). It must also include specific technical details (tools used, test conditions, results obtained) so that the tests are reproducible and verifiable without ambiguity.

IV.1.2 Dynamic test

The purpose of a dynamic test service is to verify the presence of vulnerabilities and/or functional anomalies in the gaming software by performing an analysis of the software's behaviour in accordance with assumptions expressed based on input data, the state of the software, and expected results or observations.

The dynamic test consists of running all or part of the software, under controlled and reproducible conditions for the purpose of observing the software's behaviour and highlighting a malfunction.

The dynamic test is similar to a functional test.

IV.1.3 Source code audit

The purpose of a source code audit service is to verify the presence of vulnerabilities and/or functional anomalies in the gaming software by performing an analysis of the software source code. The auditor will have to focus on issues related to the security and operational safety of the software vis-à-vis potential attacks.

The analysis shall be carried out in consideration of the following two areas of research:

- Technically, the analysis consists of validating compliance with best development practices. The auditor will then have to adapt its analyses to the particularities of the language (sensitive functions, memory management, call of external components, etc.);
- Functionally, the analysis consists of validating the correct implementation of security functions and business functions, and looking for for the presence of illegal means of circumventing these functions.

Source code audit is a service that can possibly be assisted by automated tools. However, manual analysis is still necessary.

The source code audit should at least aim to examine:

1. The client/server communication mechanism;

2. The authentication and session monitoring mechanism;
3. The authorisation and/or access control mechanism;
4. Interception vulnerabilities;
5. Injection vulnerabilities;
6. Processing of inputs/outputs;
7. Protection of sensitive data.

The analysis must clearly show relevant extracts of source code in the body of the audit report.

To ensure that the audited software is not modified, a cryptographic fingerprint of the various files will have to be provided in the report. In the presence of an imposing source code, 'directory' fingerprinting mechanisms can be provided. The fingerprinting mechanism should be clearly detailed and reproducible.

IV.1.4 Intrusive audit

The software intrusive audit combines a source code audit with an intrusion test.

This analysis is similar to a white box intrusion test, with the aim of bringing the benefits of source code audit coupled with an intrusion test. The results of the source code audit and the intrusion test must be cross-referenced to feed into each other.

The analysis of the source code must clearly show relevant extracts of source code in the body of the audit report.

IV.1.5 Differential intrusive audit

A differential intrusive audit combines the modified source code audit of the software with an intrusion test.

The auditor will focus his analysis on changes to the gaming software since it was last approved to ensure that no security issues have been introduced. The methodology must be based on the methodology described for intrusive audits.

IV.1.6 Technical architecture audit

A technical architecture audit aims to present the gaming platform as a whole and describe the operator's infrastructure(s).

This analysis should clearly depict level 3 network diagrams, complemented with auditor observations in the report. The diagrams should illustrate segmentation, server names, their roles, and, if necessary, their IP addresses. Special attention should be given to the interactions of the operator's systems with external networks or systems, as well as administrative mechanisms.

The report should highlight the elements that have been audited. The analysis of the physical environment should be based on on-site observations.

IV.1.7 Configuration audit

A configuration audit aims to verify the compliance of infrastructure elements with respect to best practices in information system security and technical requirements defined within a framework such as certification requirement matrices.

The configuration audit is intended to be non-invasive, relying on observations made by the auditor through on-site extractions.

This analysis shall be conducted on all equipment that may impact the security of the gaming platform, focusing in particular on the following elements:

1. Filtering equipment;
2. Switching or routing equipment;
3. Databases;
4. Standard network services (SSH, HTTP, DNS, etc.);
5. Relay servers;
6. Application servers (Apache, Tomcat, etc.).

However, if necessary, a sampling of equipment may be performed. The sampling shall consider the level of criticality and exposure of the audited infrastructure elements.

This analysis should take into account the role of equipment, their environment, and the operation of present applications to ensure the consistency of the actual configurations. It must clearly present relevant configuration excerpts within the body of the audit report.

IV.1.8 Synthetic risk analysis

A synthetic risk analysis aims to provide an overall view of the risks facing the gaming platform. The objective of this section is to present the auditor's "technical expert" perspective on the residual vulnerabilities of the infrastructure.

This analysis should not rely on any formalism or framework such as EBIOS or MEHARI. It is intended to be concise and synthetic.

IV.1.9 Requirements fulfilment check

The requirement fulfilment check is a deliverable aimed at covering all requirements defined in the technical requirement framework related to the certification. This section consolidates the analysis of requirements that are not addressed within other certification deliverables.

For each requirement, the auditor must justify the conclusion based, whenever possible, on analyses conducted in previous reports.

IV.2 Annex 2 – Matrix of technical requirements for certification

PSM (in French SMA) 6-month certification and annual certification are subject to separate matrices of technical requirements: (i) the 6-month certification requirements matrix and (ii) the annual certification requirements matrix.

Each matrix contains compliance and safety requirements, numbered and categorised by theme. The requirement matrices must be completed by the certifying body at the end of its analysis during the certification tasks. They summarise the results achieved through:

- The various technical analysis operations carried out by the certifying body (applicative, architectural, configuration or intrusion tests);
- Analysis of the documentation submitted by the operator;
- Integration of certificates of absence of modification produced, where appropriate, by the operator. Note: this absence of modification must not be incompatible with maintaining security (e.g. management of security updates, adaptation to new attacks through state-of-the-art strengthening measures, etc.).

The matrices are available in the accompanying document entitled 'Matrices of Technical Requirements for Certification'.

IV.3 Annex 3 – Requirements Classification Scale

A severity level, on a scale of 1 to 3 (most severe), is assigned to each requirement of the certification requirement matrices:

Severity	Description
Level 3	➢ Corresponds to requirements where non-conformity is considered to be very critical, most often in terms of regulatory compliance or security (on a exposed component and/or handling critical data).
Level 2	➢ Essentially corresponds to requirements for which non-conformity has an operational impact: failure to apply a procedure, failure to comply with the operational compliance and security requirements laid down by the National Gaming Authority, or failure to follow the rules of good practice in the security of information systems.
Level 1	➢ Essentially corresponds to the requirements related to the existence of documentation or of a procedure (e.g.: security policy, procedure for updating, strengthening a system, etc.)

Severity levels are not fixed. They may be re-evaluated by the certifying body after expert advice and possible exchange with the operator at the time of measurement of the control point. The certifying body can therefore modulate the severity of a requirement, depending on the exact nature of the non-conformity identified and in particular its contextual elements. Where appropriate, it must state very precisely what its assessment criteria are, in order to justify any deviation from the nominal level of severity of a non-conformity. For example, an application vulnerability will not have the same severity

level (2, default), depending on the exposure of the impacted component and its proximity to user data.

IV.4 Annex 4 – Vulnerability Classification Scale

Vulnerabilities are classified in accordance with the risk they pose to the information system. This risk is assessed on the basis of the impact of the vulnerability on the information system and its difficulty in operating.

The following are the different scales that the ANJ proposes to use as part of the security audits for gaming software to classify any identified vulnerabilities.

IV.4.1 Scale of impact of exploitation of vulnerability

The impact corresponds to the consequences that the exploitation of vulnerability can have on the audited information system. It is estimated using the following scale:

Level of impact	Description
Critical	➢ Generalised consequences for the information system as a whole. ➢ Breach in integrity and confidentiality of sensitive data. ➢ Exploitation of vulnerability can threaten the sustainability of the system and, more generally, the vital interests of the organisation.
Major	➢ Limited consequences for part of the information system. ➢ Confidentiality breach of sensitive information. ➢ The exploitation of vulnerability allows an attacker to compromise the security of the target and its environment, and will in fact constitute a substantial and extensive disturbance to the organisation.
Significant	➢ Isolated consequences on specific points of the information system. ➢ Breach in confidentiality of technical information about the target. ➢ Exploitation of vulnerability allows an attacker to partially compromise the security of the target and will constitute an significant disturbance to the organisation.
Minor	➢ No or little direct impact on the security of the information system if the vulnerability is exploited. ➢ Confidentiality breach of non-sensitive information.

IV.4.2 Scale of ease of exploitation of vulnerability

The ease of exploitation of a vulnerability corresponds to the level of expertise and the means necessary to carry out an attack. It is estimated using the following scale:

Ease of exploitation	Description
Easy	The exploitation of vulnerability is trivial: It requires neither specific technical competence nor special tools.
Moderate	Exploiting vulnerability requires the implementation of simple techniques and/or publicly available tools.
High	Exploiting vulnerability requires security skills in information systems and the development of simple tools.
Difficult	The exploitation of vulnerability requires expertise in the security of information systems and a high implementation cost, partly due to the development of specific and targeted tools.

IV.4.3 Vulnerability severity matrix

The level of risk associated with each vulnerability is assessed using the following value scale:

Level of severity	Description
Critical	Critical risk to the information system and requiring immediate correction or immediate termination of service.
Major	Major risk to the information system and requiring short-term correction.
Significant	Moderate risk on the information system and requiring medium-term correction.
Minor	Low risk on the information system that may require correction.

The determination of the severity level (or criticality) of the identified vulnerabilities is based on the impact and ease of exploitation of the vulnerability and is based on the following matrix:

Ease of exploitation / Impact	Difficult	High	Moderate	Easy
Critical	Significant	Major	Critical	Critical
Major	Significant	Major	Major	Critical
Significant	Minor	Significant	Significant	Major
Minor	Minor	Minor	Significant	Major

IV.5 Annex 5 – Security and recommendations for use

Under the rules and recommendations set out in the General Security Standards (RGS) established by the National Agency for the Security of Information Systems (ANSSI), the ANJ recommends the use of standards and tools in accordance with the following usages:

Usage case	Recommended standards/functions/algorithms	Recommended tools
Encryption of a file	OpenPGP standard (RFC 4880) – asymmetric encryption – RSA system (key size of at least 2 048 bits)	GNU Privacy Guard (GnuPG)
Electronic signature of a file	OpenPGP standard (RFC 4880) – asymmetrical signature – RSA system (key size of at least 2 048 bits)	GNU Privacy Guard (GnuPG)
Calculation of the cryptographic fingerprint of a file	SHA-256	sha256sum