AUTORITÉ NATIONALE DES JEUX

THE FRENCH REPUBLIC

TECHNICAL REQUIREMENTS FOR THE APPROVAL OF GAMING AND BETTING SOFTWARE

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

Under Article 34 of Law No 2010-476 of 12 May 2010, the National Gaming Authority (Autorité nationale des jeux - ANJ) approves gaming and betting software used by licensed operators or holders of exclusive rights.

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 L320-3 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. Ensuring 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 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:

"The ANJ 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 safety.

It approves, in particular with a view to ensuring compliance with the relevant gaming and betting regulations, the gaming and betting software used by operators.

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

Article L231-1 of the Public-Government Relations Code:

"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 ANJ 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 ANJ 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."

Provisions of Article 11 of the Annex to the Order of 27 March 2015 approving the specifications applicable to online gambling operators.

Provisions of the Decree No 2016-1326 of 6 October 2016 on categories of table games mentioned in section II of article 14 of Law No 2010-476 of 12 May 2010 regarding the opening-up to competition and regulation of the online gambling and games of chance sector.

I.2 Presentation and objectives of the document

Under the provisions of Article 34(VIII) 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, as amended by Ordinance No 2019-1015 of 2 October 2019 reforming the regulation of gambling and games of chance, the ANJ approves the gambling and betting software used by licensed gaming operators or holders of exclusive rights.

The purpose of the approval of the gaming software is to:

- Ensure that the gaming software complies with the rules of the game displayed by the operator to the players;
- Ensure the safety and robustness of the technical device implemented by the operator;
- In general terms, ensure that gambling software complies with the French State's gambling and betting objectives.

The actions carried out by the Authority in this context form part of the control framework it has put in place, aimed at meeting the objectives set out in Article L320-3 of the Internal Security Code. If the evaluation of an application for approval indicates that the gaming software contravenes any of these objectives, the ANJ will reject the application.

For this purpose, this document sets out the technical requirements for approval of gaming software.

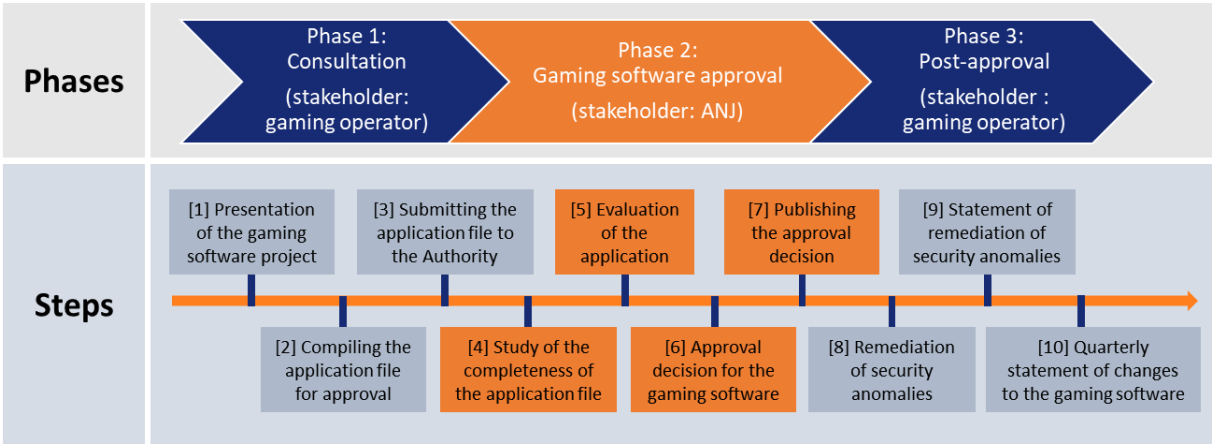
It sets forth:

- The scope of the gaming software approval procedure, i.e. in which cases the operator must apply for software approval (see Section II);
- The scope of the approval, i.e. all the elements which must be covered by the various audits included in the approval file (see Section III);
- The work and audits to be carried out prior to submitting the application (see Section IV);
- The approval procedure (see Section V);

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

- Monitoring of approved software (see Section VI).

The different phases of the approval procedure are shown in the figure below:



I.3 Glossary

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

Online gambling and bet game: gambling and bet game in which the bet is placed through the medium of an online service available over the internet.

Rules of the game: set of standards governing the running conditions of a game. The rules describe, among other things, the equipment required for the game, the number of players allowed, the purpose of the game (or conditions of victory), the game start situation and how to play the game.

Game mechanics (or game logic): in the present document, refers to the set of calculations, information processing and behaviours enabling the implementation of the rules of the game defining the game.

Game primitive: elementary game information processing function. The sequence of a coherent set of game primitives aims to constitute a game mechanics.

Business functions (of a gaming software): set of game primitives and functions which altogether contribute to the implementation of a game mechanics and game rules that constitute and define a game.

Software architecture: organisation of the various components comprised in the software.

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.

Gaming platform: all of the technical infrastructures implemented for the purpose of providing gaming services to players or gamblers.

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).

Gaming software (or gambling software): set of computer applications or programs implementing the game mechanics.

Any computer application or program supporting or modifying all or part of the game mechanics shall be considered an integral part of the gaming software.

The gaming software is conceptually composed of the following business components:

- A game engine integrated into the gaming platform;
- A totaliser for mutual betting games;
- A random number generator device (RNG) for games of chance;
- For one or more gaming clients available to players (examples: Web application, mobile apps for Android and iOS, terminal software, point-of-sale terminal software, automatic remote gaming systems;
- API[2] services, integrated into the gaming platform, enabling the various application components of the gaming platform or any other external application (including gaming customers) to interact with the game engine.

If the gaming software has been developed in accordance with modular architecture that respects the business areas described above, the software approval can be processed in modular fashion.

Game engine: gaming software component, usually integrated into the gaming platform, responsible for the provision of game primitives to the gaming software up to the complete management of gaming operations (examples: sports and horserace betting, draw and distribution of cards in poker, calculation and distribution of winnings, etc.). The advantage of a game engine developed as a separate module lies in the modular nature of the solution and the abstraction layer it offers for developing games that are based thereon. The rules of the game and game mechanics are usually carried by the game engine.

Totaliser (for mutual betting): Component of the mutual gaming software, usually integrated into the game engine, making a set of calculations, as part of a game, such as calculating the masses of stakes, the payout ratios of winning games, and winning coupons of players.

Gaming client: component of the gaming software, made available to players or gamblers, or retailers, allowing them to interact, in a "client-server" relationship, with the gaming platform, in particular the game engine (examples: consultation of the gambling offer posted by the operator, betting placement, consultation of betting results and associated winnings).

The gaming client can implement all or part of the game mechanics and appear in different forms:

- Web application, accessible from the operator's website using a web browser;

[2] API: Application Programming Interface. Solution that allows applications to communicate with each other and exchange services or data, *via* a programming language.

- Computer application in the form of a thick client to be installed on the user's station;
- Application for mobile devices or tablets;
- Application for point-of-sale terminals;
- Automatic remote gaming processing system (e.g.: betting software via SMS or instant messaging).

It must be noticed that the gaming client is conceptually distinct from the software client being used. For instance, in the case of a smartphone app, the software client comprises the gaming client may also offer other services such as gamer account management, game statistics, news and so forth. The approval of the gaming client does not aim to cover the services provided beyond the gaming client, it must however check that the gaming client is adequately isolated from the other services in terms of software security.

(Automatic) terminal, also known as game terminal without human intermediation: hardware device, positioned in a physical distribution network (examples: racetracks, retailers, tobacconists), integrating a software interface of the type of gaming client, directly accessible to players or gamblers. This device enables the game to be played, the results of a game and the associated winnings to be consulted. It also authorises payment transactions (feeding and withdrawal of money) under conditions previously brought to the knowledge of the players.

Point-of-sale terminal, also known as game terminal with human intermediation: the point-of-sale terminal has the same functions as the point-of-sale terminal, however, access to the software interface is restricted to the personnel authorised by the operator and responsible for the point of sale (examples: retailers, tobacconists). The terminal may offer other functions for the retailers to use (stock management, cash management, ticket sales…)

Internet terminal: the player's means of accessing the Internet. This is generally a computer but may also be a telephone, tablet, etc., providing that the means gives the player direct access to the website.

Random Number Generator (RNG): device capable of generating a sequence of values with random (or close to random) properties, for which it is difficult, if not impossible, to identify groups of numbers that follow identifiable prediction rules.

This device is implemented when the course of the game requires the generation of a random element, for example, in poker with the random draw of cards or even online lottery games without a physical draw.

I.4 Identification of requirements and recommendations in the document

This document has two levels of recommendations:

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

II Scope of the gaming software approval procedure

The following requirements define the framework to determine when it is relevant to request a gaming software approval. Software approval is required in the following cases:

[E_HOM_CHA1] New gaming software or a new component of a gaming software must systematically be approved before the commissioning thereof. This rule applies to approvals requested (i) in the context of filing an application for licensing, but also (ii) where an operator regulated by the ANJ wishes to operate a new game.

[E_HOM_CHA2] Gaming software or component of the gaming software specific to a new media (examples: mobile phone, tablet, etc.) is considered a new gaming software.

[E_HOM_CHA3] Gaming software that has been the subject of a substantial development, since its last approval, is considered new gaming software.

What is a substantial development?

A development qualifies as substantial when either:

1. It modifies the game mechanics;
2. It modifies the game rules;
3. It questions the validity of the audit of the security of the gaming software.

The audit of the security of the gaming software may be questioned when the development encompasses one or more of the following points:

4. Any development of the gaming software modifying all or part of the mechanisms or configurations directly affecting the security of the gaming software (examples: authentication, session management, client-server encryption);
5. Any modification of the internal architecture of the gaming software (i.e. adding or suppressing one or more components);
6. Any technical developments corresponding to the replacement of a technology integrated into the gaming software by another (examples: framework, software library, programming language) with the exception of version upgrade;
7. Any changes to infrastructure altering the gaming software exposition in terms of security (examples: change of the hosting site, the host or the gaming platform provider);
8. Any technical developments relating to the addition or modification of direct interconnections of gaming software with other information systems.

Provided they do not fall under the provisions referred to under No 1,2 and 3, the following developments will not be classified as substantial:

9. Version upgrade of the gaming software or one of its components;
10. Fixes of bugs and potential vulnerabilities;
11. Any modification of the graphic chart of the interface or the ergonomy of the gaming software accessible to players.

Should there be any doubt as to the compliance with the objectives of the State's gambling and betting policy as set by article L. 320-3 of the Internal Security Code, the ANJ reserves the right to requalify an evolution as substantial on the occasion of quarterly follow-ups (see Section VI.1) and annual certifications (see Section VI.2). The Authority may therefore require an operator to apply for the approval of a software if it appears that the development in question qualifies as substantial.

[E_HOM_CHA4] Gaming software, or a component thereof, which has been decommissioned (i.e. out of operation) for more than 12 months, is considered by the Authority as new gaming software if the operator decides to put it back into service.

[E_HOM_CHA5] Approved gaming software must be put into production within 12 months of the date of approval. In addition, the operation of the gaming software is conditional on obtaining a new approval, unless the Authority expressly advises otherwise.

[E_HOM_CHA6] The operation by an operator, for its own gaming or betting activity, of a gaming software already approved for the benefit of another operator is subject to re-approval.

The scope of the gaming software approval may be restricted to the sole audit of security of the gaming software, provided it has not been subject to any substantial development since its last approval.

[E_HOM_CHA7] A terminal or point-of-sale software, allowing players direct or indirect access (*via* for example a tobacconist) to a gambling game, is considered a component of the gaming software. Its operation is conditional upon obtaining approval.

[E_HOM_CHA8] Software for printing physical scratch game tickets subject to exclusive rights, is considered part of the operator's gaming equipment. This software is therefore subject to approval.

III Scope of audits

[E_HOM_PER1] The scope of the approval of the gaming software includes solely the considered gaming software. The audit of security must however be able to offer guaranties regarding the absence of security impacts to the gaming software stemming from the other components of the platform. The scope of the security audit of the gaming software may therefore need to be extended adequately to meet this requirement.

[E_HOM_PER2] The scope of the security audit is defined considering:

- Recommendations, reservations and remediation plans resulting from previous registrations for previously approved gaming software;
- Interconnections of gaming software with other information systems;
- The means and procedures used for the maintenance of gaming software in secure condition (MCS);
- The means and procedures used for the maintenance, operation and remote management of the information system, particularly when carried out by external service providers (e.g.: B2B partnership between an authorised operator and a gaming platform provider for online poker gaming activities).

The adoption of a modular approach of the gaming software may be considered in the context of an approval. The scope of the application may then be restricted:

- either to exclusively new components of the gaming software that have not yet been approved;
- or to those components already approved for the gaming software that have undergone substantial development since the last approval.

For example, a new gaming client will be eligible for approval on its own, without the need to re-approve the already-approved game engine on which the game is based, provided that the game has not undergone a substantial development since it was last approved.

[E_HOM_PER3] The limitation of the scope of the application for approval of gaming software to only part of its components shall be explained and justified by the operator in the approval application file.

Important information:

The operator must not operate gaming software before it is approved by the ANJ. An operator who fails to recognise the prior nature of the approval commits a breach which could lead to the opening of a sanction procedure under Article 43 of Law No 2010-476 of 12 May 2010 as amended. In addition, the ANJ will be able to ask the operator to stop the operation of this software without delay, which should be regarded as taking place at the operator's own risk.

Recommendation:

In case of doubt as to the need for approval, the scope of the approval or any other questioning, operators are invited to approach the ANJ before the possible submission of the file.

This exchange may also make it possible to discuss the legal conformity of the draft.

IV Work prior to filing the application for approval

Where gaming software approval is required, the operator must arrange a certain number of audits (see Sections IV.2, IV.3 and IV.4) and establish an remediation plan based on the conclusions thereof.

IV.1 Provisions common to the various audits

IV.1.1 Conducting audits

[E_HOM_AUD1] The various audits requested as part of the approval of a gaming software are carried out by one or more third-party auditors.

[E_HOM_AUD2] The operator is required to provide the ANJ with a copy of the audit performance contracts in the approval application file.

[E_HOM_AUD3] These various audits shall be performed in the 12 months preceding the filing of the application for approval. The end date of the audit performance shown in each of the various audit reports ensures that this deadline is met.

The operator's attention is drawn to the fact that failure to comply with this obligation relating to the seniority of audits is a reason for the incompleteness of the approval application.

[E_HOM_AUD4] Each audit report shall be signed electronically by the auditor, in accordance with the standard set out in Annex 4 to this document. The electronic signature files obtained then accompany the various audit reports attached to the approval application file.

To verify the authenticity of the audit reports, the auditors will communicate to the ANJ, prior to the submission of the application for approval, their public key *via* the contact email address: regulation-si@anj.fr.

[E_HOM_AUD5] Each resource audited or used to support an audit, (1) of the type documentary resource, e.g. game regulation or technical annexes, or (2) of the type source code, delivered to the auditor by the operator as part of an audit, is attached to the approval application file.

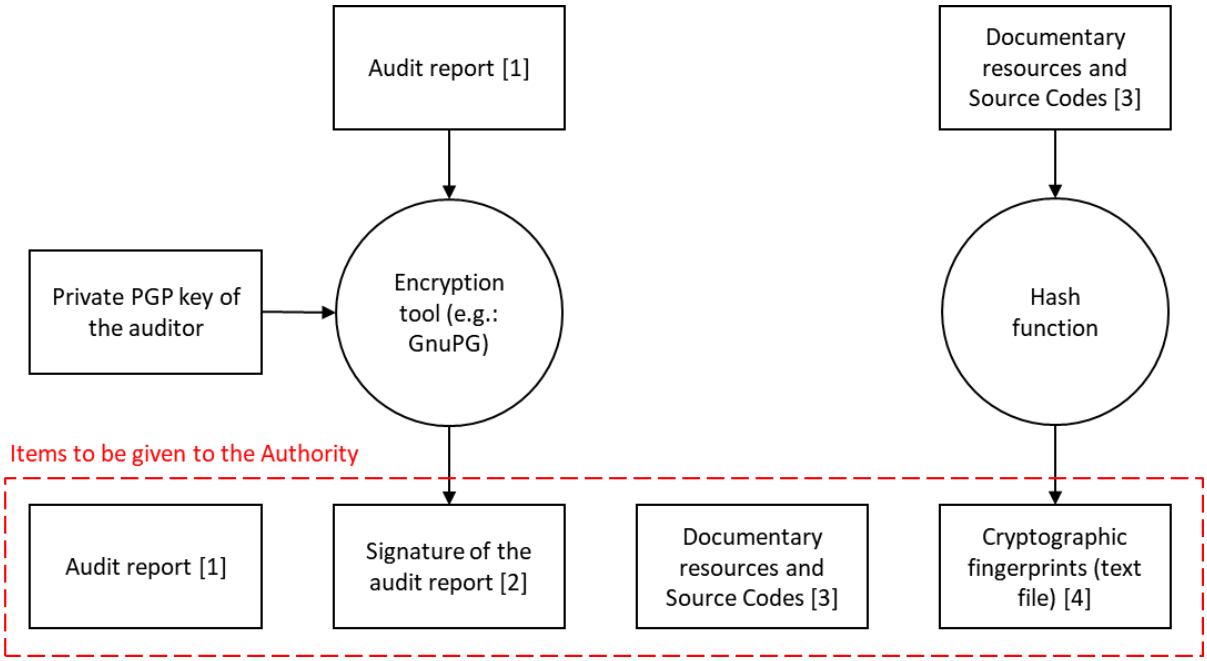
The source code may be directly transmitted by the provider, should the operator not be granted access to it.

In the case neither the provider nor the operator can communicate the source code to the Authority, security audits/functional audits of the source code must be provided to the ANJ, along with the legal provisions binding the operator and its provider regarding the security of provided service and the security of the gaming software.

[E_HOM_AUD6] The resources used in an audit must be the subject of a cryptographic fingerprint calculation. This calculation is carried out by the auditor using the hash function indicated in Annex 4 to this document. The resulting fingerprints are compiled in a text file accompanying the audit report prepared by the auditor. The cryptographic fingerprint of the text file must also appear in the audit reports.

All of these cryptographic fingerprints must ensure that the resources submitted to the Authority as part of an application for the approval of gaming software correspond to the resources audited or used to support an audit.

Refer to the schematic diagram below:



IV.1.2 Non-conformities and security anomalies

[E_HOM_CAN1] Prior to the filing of the application for approval, any non-conformities, identified during the audit of the conformity of the implementation of the business functions within the gaming software, (i) have been remedied, (ii) the corrections provided have been validated by the auditor and (iii) this validation has been documented in the audit report attached to the file of the application for approval.

[E_HOM_CAN2] Prior to the filing of the application for approval, any possible security anomalies qualified as major or critical[3], identified in the audit of the security of the gaming software, (i) have been remedied, (ii) the corrections provided have been validated by the auditor and (iii) this validation has been documented in the audit report attached to the file of the application for approval.

[E_HOM_CAN3] Possible security anomalies qualified as minor or significant, identified during the security audit of the gaming software, must be the subject of (i) a remediation plan. Their correction is not required prior to the approval decision for the gaming software, but it must take place within a period of (ii) not more than 12 months for minor anomalies (iii) no more than 6 months for significant ones from the date of the approval decision. These corrections must be validated in the annual certification process.

[E_HOM_CAN4] If there is no security measure that directly corrects security anomalies, the operator will have (i) to propose compensatory measures to avoid their exploitation. The proposed

[3] Refer to the vulnerability severity scale defined in Annex 3 to this document.

compensatory or perimeter protection measures for major or critical security anomalies shall (ii) be put in place and (iii) validated by the auditor, prior to the submission of the application for approval. (iv) This validation shall be documented in the relevant audit reports attached to the application file.

[E_HOM_CAN5] When submitting the application for approval, the operator shall justify to the ANJ any refusal to correct security anomalies and non-conformities identified during the various audits 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.

IV.1.3 Remediation plan

[E_HOM_PRM1] The operator shall draw up a remediation plan comprising, for each security anomaly or non-conformity identified in the audit reports, a record of at least three parts:

1. A synthetic description of the anomaly or non-conformity. In the case of a security anomaly, the associated level of risk (see annex No 2) should also appear on the record;
2. The auditor's recommendations to correct the anomaly or non-compliance;
3. The action plan justifying the operator's management of the anomaly or non-conformity. This plan details the actions taken or planned by the operator to correct the anomaly or non-conformity (including compensatory measures) and specifies the timetable for carrying out these actions.

[E_HOM_PRM2] For minor and significant security anomalies, the operator is required to report to the ANJ on the implementation of the remediation plan on the dates indicated.

IV.2 Provisions for the audit of the security of the gaming software or component to be approved

This audit ensures that the security implemented at the level of the gaming software or component to be approved is "state of the art" or close to it.

[E_HOM_SEC1] The intrusive audit report will follow the detailed plan below. It may contain additional sections if the operator or auditor deems it necessary:

Conditions for conducting the audit:

1. The name and contact details of the body responsible for carrying out the audit;
2. Information on the stakeholders (name, first name, occupation, contact address);
3. The start and end dates of the audit performance;
4. The person responsible for carrying out the audit;
5. A list of the items made available to the auditors;

Scope of the audit:

6. A description of the scope of the audit. It also includes a list of audited application modules and associated versions;
7. The cryptographic fingerprint of the audited source code files to ensure that the audited software is not modified;
8. The cryptographic fingerprint of the documentary resources under scrutiny or used for the audit;

Methods:

9. An explicit description of the methodology used in the audit to detect and exploit vulnerabilities where appropriate (e.g.: white box/grey mode analysis, manual/automated source code analysis, search for sensitive points of language and technology used, analysis of configuration files, search for potentially dangerous entry points;

Managerial synthesis:

10. The auditor's opinion concerning the level of safety of the gaming software or component to be approved;
11. Synthesis of positive points;
12. Synthesis of identified vulnerabilities and associated risks;
13. Synthesis of the auditor's recommendations to address identified vulnerabilities;

Validation of corrections:

14. The auditor's opinion on corrections and other compensatory measures applied by the operator to identified vulnerabilities, in particular major or critical vulnerabilities;

Presentation of the gaming software or component to be approved:

15. A reminder of the functional description of the software, the application architecture and the interactions between the different software packages;

Detailed analysis:

16. Identification of security needs: this section will present the required security features (e.g.: authentication, session management, sensitive data storage, password policy, prevention against known attacks: XSS, CSRF, SQL Injection, denial of service, etc.);
17. Validation of the security features and the proper implementation of security measures to meet the needs mentioned in the previous point: this part will describe the various security mechanisms and their implementation in the source code of the gaming software or component for approval (communication security, use of anti-CSRF tokens, validation of exchanged data, robustness of hash and encryption algorithms used, etc.);
18. Looking for vulnerabilities outside security features: this part should specify whether the application is vulnerable to other types of attacks, not dealt with in the previous point (e.g.: default configuration, use of an obsolete version of a dependency, etc.);

19. The auditor's recommendations to address identified vulnerabilities and improve software security (e.g.: best development practices).

[R_HOM_SEC1] As part of the development of gaming software or the component for approval, which has already been approved, the scope of the audit may be restricted only to changes that have been made since the last approval. It will therefore be necessary to carry out a differential intrusive audit (see Annex 2).

IV.3 Provisions for the audit of the quality and safety of the random number generator

This audit ensures that the level of quality and security of the RNG device is sufficient to meet the objective of integrity of the game operations prescribed in Article L320-3(2) of the Internal Security Code.

[E_HOM_GNA1] The RNG device audit report will follow the detailed plan below. It may contain additional sections if the operator or auditor deems it necessary:

Conditions for conducting the audit:

1. The name and contact details of the body responsible for carrying out the audit;
2. Information on the stakeholders (name, first name, occupation, contact address);
3. The start and end dates of the audit performance;
4. The person responsible for carrying out the audit;
5. A list of the items made available to the auditors;

Scope of the audit:

6. A description of the scope of the audit. The aim is also to present the list of audited application source codes, the RNG and source codes transforming the generated random numbers into game chance.
7. The cryptographic fingerprint of the audited source code files to ensure that the audited application source codes are not modified;
8. The cryptographic fingerprint of the documentary resources under scrutiny or used for the audit;

Methods:

9. A description of the quality and safety audit procedure for the RNG.

Managerial synthesis:

10. The auditor's opinion on the quality and safety of the RNG;
11. Synthesis of positive points;
12. Synthesis of identified vulnerabilities and associated risks;

13. Synthesis of the auditor's recommendations to address identified vulnerabilities;

Validation of corrections:

14. The auditor's opinion on corrections and other compensatory measures applied by the operator to identified vulnerabilities, in particular major or critical vulnerabilities.

Presentation of the RNG device:

15. A description of the context of use of the RNG (e.g.: drawing of cards in poker);
16. General description of the RNG. This includes presenting the architecture of the device and the technologies used;
17. A description of the hardware platform associated with the RNG device;

Detailed analysis:

18. Analysis of the operator's documentation (including functional and technical description) relating to the RNG device. The aim is to verify whether such documentation exists, whether it is up-to-date, and its editorial quality;
19. Validation of technological choices (software, hardware, architecture) in relation to the context of use of the RNG device;
20. Analysis of the initialisation and refreshing process of the RNG (type and quality of sources of random elements, seed entropy, frequency of generator refreshing);
21. Analysis of the RNG algorithm;
22. Analysis of the use of random numbers in the gaming platform (e.g.: analysis of the card mixing algorithm used as part of poker games);
23. Validation of the mechanism guaranteeing the integrity of the generator over time (e.g.: regular verification of the signature of binaries of the application source codes constituting the RNG;
24. Validation of the control process ensuring the stability through time of the actual randomness of the generated numbers (e.g.: statistical tests carried out on a periodic basis, accompanied by an anomaly management procedure;
25. The auditor's recommendations to address identified vulnerabilities and to improve the security and quality of the RNG.

IV.4 Provisions for auditing compliance of implementation of business functions

This audit ensures that the implementation, at the level of the software or component to be approved, of the business functions relating to the rules of the game and the game mechanics (including the rules of calculation, the game primitives and, in general, the behaviour of the software) complies with the rules of play as presented, literally, to the players and with the course of the game as presented on the site or application that is the medium of the gaming offer.

It also ensures that there is no reasonable way to circumvent these rules.

[E_HOM_CFM1] The business function audit report will follow the detailed plan below. It may contain additional sections if the operator or auditor deems it necessary:

Conditions for conducting the audit:

1. The name and contact details of the body responsible for carrying out the audit;
2. Information on the stakeholders (name, first name, occupation, contact address);
3. The start and end dates of the audit performance;
4. The person responsible for carrying out the audit;
5. A list of the items made available to the auditors;

Scope of the audit:

6. A description of the scope of the audit;
7. The cryptographic fingerprint of the audited source code files to ensure that the audited software is not modified;
8. The cryptographic fingerprint of the documentary resources under scrutiny or used for the audit (example: game rules, technical annexes, contracted requirements);

Methods:

9. A description of the audit procedure for the business functions and their implementation in the source codes of the audited software;

Managerial synthesis:

10. The auditor's opinion on the level of compliance of business functions;
11. Synthesis of identified non-conformities;
12. A synthesis of the auditor's recommendations to correct non-conformities;
13. The auditor's opinion on the corrections made by the operator to the identified non-conformities;

Validation of corrections:

14. The auditor's opinion on the corrections and other countervailing measures applied by the operator to the identified non-conformities;

Detailed analysis of business functions and their implementation:

15. For circle games:
    a) The rules of the game as displayed to the players and their analysis;
    b) Analysis of the proposed poker game variants;

c) Analysis of gambling offers: tournaments, cash games, sit&go and other possible game formats;

d) Analysis of the management of a player's registration in a game (including tournaments);

e) Analysis of gambling actions (placement of players, increase of blinds, distribution of cards, distribution of winnings, etc.);

f) Analysis of information displayed to players (game history, current games, results, stakes and winnings);

16. For sports betting:

a) The rules of the game as displayed to the players and their analysis;

b) Analysis of gambling actions (recording bet, unbundling, distribution of winnings, etc.);

c) Analysis of information displayed to players (game history, betting and running games, results, stakes and winnings);

17. For horserace betting:

a) The rules of the game as displayed to the players and their analysis;

b) Analysis of gambling actions (recording bet, unbundling, distribution of winnings, etc.);

c) Analysis of information displayed to players (game history, betting and running games, results, stakes and winnings);

18. For lottery games:

a) Analysis of the rules of the game displayed to players;

b) Analysis of the gambling actions (game playing, unwinding, distribution of winnings, etc.);

c) Analysis of information displayed to players (game history, current games, results, stakes and winnings);

19. In the specific case of a game engine:

a) Analysis of all game primitives;

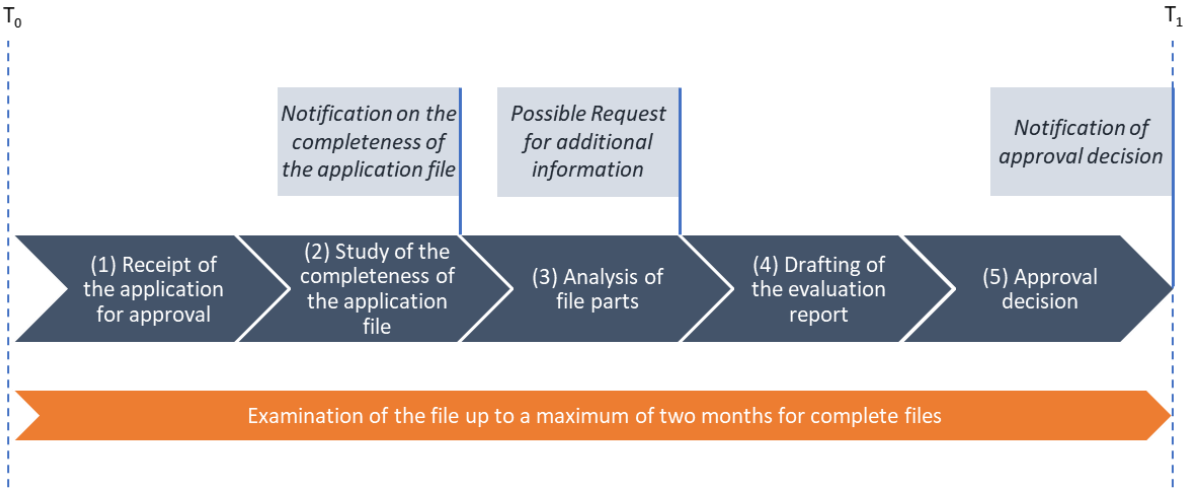
20. In the specific case of a totaliser for mutual betting:

a) The analysis of the calculation rules with particular regard to the masses of stakes, the ratios and the distribution of winnings;

21. Searching for means of circumvention rules of the game, calculation rules and game mechanics implemented at software source code level.

V Procedure for the approval of gaming software

The diagram below presents the different stages of the evaluation of an application for approval.



V.1 Contents of the file

[E_HOM_PDH1] The application file for the approval of gaming software filed with the ANJ, in a paperless format, includes the following parts:

V.1.1 Case of the approval of an online game

Generally, the application file for gaming software associated with an online game includes:

1. The application form for the approval of the gaming software, duly provided. This form is made available on the ANJ website[4];
2. The functional and technical description of the gaming software and, where applicable, its evolution;
3. The gaming software security audit report (see Section IV.2);
4. The audit report certifying that the rules of the game and the game mechanics implemented in the gaming software are compliant with the game as it is presented to the player (see Section IV.4);
5. The rules of the game, describing the rules of play and accompanied by any general conditions of use;
6. The plan for the remediation of anomalies and non-conformities found during the gaming software audit (see Section IV.1.3);
7. The source code of the gaming software submitted for approval or its substitutes as defined in the requirement [E_HOM_AUD5].

[4] Link: https://anj.fr/regulation/documentation-destination-des-operateurs

If the game is based on a RNG device that is not already approved, it must be subject to specific approval (see Section IV.3).

If the game is based on a game engine that has already been independently approved, the scope of the approval may be restricted to other components of the gaming software that have not yet been approved or which have undergone substantial development since the last approval.

V.1.2 For approving a RNG device

The random number generator (RNG) on which a game relies is subject to independent approval of the gaming software. This mode allows the re-use of the RNG for another game without the need to re-approve the RNG component, provided that the RNG component has not undergone a substantial development since it was last approved.

The operator's attention is drawn to the fact that the approval of the RNG device is not valid for the gaming software and its components.

The application package shall include:

1. The application form for the approval of the gaming software, duly provided. This form is made available on the ANJ website[5];
2. The functional and technical description of the RNG device and, where appropriate, its evolution;
3. Justification for the technological choices (software and hardware, architecture) implemented;
4. The quality and safety audit report of the RNG device (see Section IV.3);
5. The plan for the remediation of anomalies found during the audit of the RNG system (see Section IV.1.3);
6. The application source code and algorithm of the RNG submitted for approval or its substitutes as defined in the requirement [E_HOM_AUD5].

V.1.3 For game engine approval

The game engine on which a game relies may be subject to independent approval of the gaming software. This mode allows the reuse of the same game engine for another game, by reducing the approval of the software associated with the second game.

The operator's attention is drawn to the fact that the approval of the game engine is not valid for the gaming software and its components.

The application package shall include:

1. The application form for the approval of the gaming software, duly provided. This form is made available on the ANJ website[6];

[5] Link: https://anj.fr/regulation/documentation-destination-des-operateurs
[6] Link: https://anj.fr/regulation/documentation-destination-des-operateurs

2. The functional and technical description of the game engine and, where appropriate, its evolution. This documentation should also detail the available game primitives;
3. The game engine safety audit report (see Section IV.2);
4. The audit report of the proper implementation of game primitives (see Section IV.4);
5. The plan for the remediation of anomalies and non-conformities found during audits (see Section IV.1.3);
6. The source code of the game engine submitted for approval or its substitutes as defined in the requirement [E_HOM_AUD5].

If the game engine relies on a RNG device that is not already approved, this one shall be subject to specific approval (see Section IV.3).

V.1.4 For approving a totaliser for mutual betting

The totaliser used for mutual betting and on which a game relies may be subject to independent approval of the gaming software. This mode allows the reuse of the same totaliser for another game, by reducing the approval of the software associated with the second game.

The operator's attention is drawn to the fact that the approval of the totaliser is not valid for the gaming software and its components.

The application package shall include:

1. The application form for the approval of the gaming software, duly provided. This form is made available on the ANJ website[7];
2. The functional and technical description of the totaliser and, where appropriate, of its developments. Such documentation shall include details of the calculations that may be carried out by the totaliser;
3. The security audit report for the totaliser (see Section IV.2);
4. The audit report on the proper implementation of the calculation rules, focusing in particular on the masses of stakes, the reports and the distribution of winnings (see Section IV.4);
5. The plan for the remediation of anomalies and non-conformities found during audits (see Section IV.1.3);
6. The source code of the totaliser submitted for approval or its substitutes as defined in the requirement [E_HOM_AUD5].

V.1.5 For approving point-of-sale or automatic terminal gaming software

Gaming software on open access terminals or point-of-sale terminals is subject to independent and specific approval.

[7] Link: https://anj.fr/regulation/documentation-destination-des-operateurs

The operator's attention is drawn to the fact that the approval of the terminal or point-of-sale gaming software is not reduced to software elements physically installed at the point of sale but also includes in its scope the components on the operator's central platform(s) with which the terminal exchanges data, in particular, interconnection components, components taking part in the game mechanics and in the terminal software update mechanics. Should any components be considered as providing game engine services, they may be subjected to an independent approval (see section V.1.3).

The application package shall include:

1. The application form for the approval of the gaming software, duly provided. This form is made available on the ANJ website[8];
2. The technical and functional description of the gaming software and, where applicable, its developments. Such documentation shall also include the hardware device (terminal) on which the gaming software is installed and detail the means of security, both hardware and software, implemented at the terminal or point-of-sale level;
3. The security audit report for point-of-sale gaming software (see section IV.2);
4. The audit report certifying that the rules of the game and the game mechanics implemented in the point-of-sale gaming software are compliant with the game as presented to the player (see Section IV.4);
5. The game regulations, in draft or final version, describing the rules of play and accompanied by any general conditions of use;
6. The plan for the remediation of anomalies and non-conformities found during the gaming software audit (see Section IV.1.3);
7. Source code for point-of-sale gaming software.

V.1.6 For approving scratch card game ticket printing software

The software for printing physical scratch cards is subject to independent and specific approval as it carries the rules of play and game mechanics when printing the tickets.

The operator's attention is drawn to the fact that the approval of the scratch card game ticket printing software is not required for each new scratch game so long as the printing software does not undergo a substantial development for this very game.

The application package shall include:

1. The application form for the approval of the gaming software, duly provided. This form is made available on the ANJ website[9];
2. A description of the ticket generation procedure and ticket printing device;
3. A description of the printer's qualification process;

[8] Link: https://anj.fr/regulation/documentation-destination-des-operateurs
[9] Link: https://anj.fr/regulation/documentation-destination-des-operateurs

4. The presentation of the safety elements presented in the qualification file which led to the retention of the printer;
5. The presentation of contractual clauses available to the gaming operator in respect of its printers, relating to the security of the printing device and its auditability;
6. Audit reports of printers covering (i) the printing software and its functionalities, (ii) the quality of the RNG on which the printing software relies to produce the tickets and (iii) the means of securing the printing device;
7. The plan for the remediation of anomalies found during the audits.

V.1.7 Common provisions

[E_HOM_PDH1] It is up to the gaming operator to ensure, where appropriate, that the company that makes available a platform or software communicates to the ANJ all the elements necessary for the evaluation of the application.

[E_HOM_PDH2] The absence of a required part in an application file for the gaming software must be duly justified. Otherwise, the file will be considered incomplete.

[R_HOM_PDH1] In case of doubt, it is recommended that the ANJ be consulted prior to the filing of any application for approval of the gaming software to avoid suspension of the evaluation of the file, due to incompleteness of the file.

V.2 Procedures for sending deliverables

[E_HOM_TRF1] The application file is to be submitted to the ANJ through the secure exchange channel made available to operators.

However, the sending of source codes on physical USB flash drives is possible exceptionally, in which case the source codes will have to be encrypted and transmitted in accordance with the procedure the ANJ has indicated to the operator.

V.3 Evaluation of the application

The ANJ has two months to consider the application for approval.

Where the application for the approval of gaming software is made by an online gaming or betting operator, silence for two months on the part of the ANJ regarding this application constitutes a decision to reject Article 1(2) 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.

In other cases, the provisions of Article L231-1 of the Code of Relations between the Public and the Administration shall be applied.

Where the application file is incomplete, a letter shall be sent to the operator asking them to remedy it within a period of not less than 10 calendar days. The evaluation shall be suspended until the date of receipt of the supplementary material requested. The period of two months after which, in the

absence of an express decision, the application is deemed to have been accepted or refused runs only from the date of receipt of the required documents and information.

In the course of the evaluation, the applicant is required to provide, at the request of the ANJ, any information that is lawfully justified and capable of illuminating the latter with respect to the material contained in the file submitted.

Decisions on the approval of the gaming software are notified to the operator and published on the ANJ website.

Where the application for approval is made in the context of an application for licensing under Article 11(3) of the Order of 27 March 2015 approving the specifications applicable to online gaming operators, the ANJ shall issue a decision on the application for approval of gaming software separate from that relating to the application for licensing.

VI Life cycle requirements for approved gaming software

VI.1 Life cycle

[E_HOM_LOH1] The authorised or exclusive gaming operator will address at the end of every quarter, through the secure exchange channel made available by the ANJ, a list of changes made during the past three months to the various approved software available to it.

A quarterly statement of changes to approved software is made available on the ANJ website[10] and specifies all the information requested.

[E_HOM_LOH2] The operator is required to ensure the security and robustness of its gaming software when it is put into operation. The operator is therefore expected to implement all the measures to meet this objective (examples: regular security audits, software security maintenance, management of the deployment of patches, principle of defence in depth, etc.).

[E_HOM_LOH3] If the operator plans to decommission (i.e. remove from operation) approved gaming software or any of its components, it is required to inform the ANJ services within two months of the decommissioning of the software.

VI.2 Links between software approvals and annual certification

[E_HOM_CERT1] All changes made over the past year to the range of approved gaming software available to an operator are audited as part of the annual certifications.

[E_HOM_CERT2] Vulnerabilities identified at the level of gaming software during annual certification audits will have to be corrected or use of the software shall be rendered impossible within no longer than 12 months from the date the certification reports have been filled to the Authority.

[10] Link: https://anj.fr/regulation/documentation-destination-des-operateurs

VII ANNEXES

VII.1 Annex 1 – Examples of scenarios relating to the approval of software

Below are some scenarios relating to the approval of gaming software.

Scenario No 1: new licensing

Initial situation:	➢ The applicant operator has just filed with the ANJ an application for licensing for the poker activity.
Obligations of the operator:	➢ The gaming software that is the medium for the poker offer of the applicant operator is considered, by default, by the Authority, as unapproved for this applicant. The latter is required to have the poker software and the RNG device approved prior to their entry into operation; ➢ Auditors will focus their attention on the security of the gaming software and the RNG device, and on the conformity of the implementation of the game rules and the game mechanics.
Main requirements:	➢ Scope of application: **[E_HOM_CHA1]** ➢ Poker Software: **[E_HOM_SEC1], [E_HOM_CFM1]** ➢ RNG component: **[E_HOM_GNA1]**
Need for gaming software approval?	➢ YES
Contents of the approval application file	☑ The gaming software approval application form, provided; ☑ Functional description of the gaming software and its developments; ☑ Technical description of the gaming software and its developments; ☑ Functional description of the RNG and its developments; ☑ Technical description of the RNG and its developments; ☑ The justification for the technological choices implemented for the RNG; ☑ The gaming software security audit report; ☑ RNG quality and security audit report; ☑ The compliance audit report implementing the business rules; ☑ The gaming regulation displaying the rules of the game; ☑ The remediation plan; ☑ The source codes of the gaming software; ☑ Source codes of the RNG device.

Scenario No 2: new game added to already approved gaming software

Initial situation:	➢ The gaming operator has horserace betting software, already approved, composed of: ○ A game engine for managing bets, incorporating a totaliser for calculating the masses of stakes and ratios; ○ A web-based betting app (desktop and mobile sites); ○ API services relaying player requests, *via* the web-based betting app, to the game engine.
Description of the development:	➢ The gaming operator has upgraded their gaming software to expand their horserace betting offer by adding a new mutual betting game. ➢ The game engine, totaliser and web betting app have been modified to incorporate the new game into the existing game offering. ➢ The rules of the game have been updated to display the new rules of the game associated with this new betting game.
Obligations of the operator:	➢ As a new betting game involving new rules of the game and a new implementation in terms of the source codes of the game engine, the totaliser and the web betting app, the development of the gaming software is considered by the Authority to be a substantial development of horserace betting software. ➢ The scope of the audits should include, at a minimum, the modified components of the gaming software (i.e. the game engine, the totaliser and the web betting app). ➢ Auditors will focus their attention on the security of the gaming software and the conformity of the implementation of the new rules of the game and associated game mechanics. They will also check the correct implementation of the calculation rules inherent to the totaliser.
Main requirements:	➢ Scope of application: **[E_HOM_CHA1], [E_HOM_CHA3]** ➢ Horserace betting software: **[E_HOM_SEC1], [E_HOM_CFM1]**
Need for gaming software approval?	➢ YES
Contents of the approval application file	☑ The gaming software approval application form, provided; ☑ Functional description of the gaming software and its developments; ☑ Technical description of the gaming software and its developments; ☐ Functional description of the RNG and its developments; ☐ Technical description of the RNG and its developments; ☐ The justification for the technological choices implemented for the RNG; ☑ The gaming software security audit report; ☐ RNG quality and security audit report; ☑ The compliance audit report implementing the business rules; ☑ The gaming regulation displaying the rules of the game; ☑ The remediation plan; ☑ The source codes of the gaming software; ☐ Source codes of the RNG device.

Scenario No 3: new mobile application.

Initial situation:	➢ The gaming operator has a horserace betting software, which is already approved, composed of: ○ A game engine for betting management, incorporating a totaliser for calculating the masses of stakes and ratios; ○ A web-based betting app (desktop and mobile site); ○ A mobile app for iOS; ○ API services relaying player requests, *via* web and mobile betting apps, to the game engine.
Description of the development:	➢ The gaming operator wishes to extend access to its horserace betting offer to players with a mobile device for Android. A new mobile app for Android has therefore been developed. ➢ Mobile apps for Android and iOS share the same source code base. ➢ The rules and mechanics of the game are not changed. ➢ The gaming platform integrating the game engine, totaliser, web application and API services remains unchanged.
Obligations of the operator:	➢ As a new gaming medium, the mobile app for Android will need software approval. ➢ The scope of audits should include, at a minimum, the new mobile app for Android. ➢ Auditors will focus their attention on the security of the mobile app for Android and communication channels linking this application to the gaming platform. ➢ The auditors will also analyse the conformity of the implementation of the rules of the game and logic, in particular through the execution of dynamic tests from the new mobile application.
Main requirements:	➢ Scope of application: **[E_HOM_CHA1], [E_HOM_CHA2]** ➢ Scope of the audit: **[E_HOM_PER3]** ➢ Horserace betting software: **[E_HOM_SEC1], [E_HOM_CFM1]**
Need for gaming software approval?	➢ YES
Contents of the approval application file	☑ The gaming software approval application form, provided; ☑ Functional description of the gaming software and its developments; ☑ Technical description of the gaming software and its developments; ☐ Functional description of the RNG and its developments; ☐ Technical description of the RNG and its developments; ☐ The justification for the technological choices implemented for the RNG; ☑ The gaming software security audit report; ☐ RNG quality and security audit report; ☑ The compliance audit report implementing the business rules; ☑ The gaming regulation displaying the rules of the game; ☑ The remediation plan; ☑ The source codes of the gaming software; ☐ Source codes of the RNG device.

Scenario No°4: application redesign

Initial situation:	➢ The gaming operator has already-approved poker gaming software, including: ○ A poker game engine; ○ A poker gaming web application (desktop and mobile site); ○ A mobile app for iOS; ○ A mobile app for Android; ○ API services relaying player requests, *via* web and mobile applications, to the game engine.
Description of the development:	➢ The operator performed a redesign of their poker game engine. It plans to replace its already approved but ageing game engine with a new, fully redeveloped game engine. The application redesign is done at iso-functionality of the old game engine. ➢ The rules and mechanics of the game are not changed. ➢ With the exception of the game engine, the other components of the gaming software remain unchanged. ➢ The RNG device, which is already approved, is not affected by this redesign.
Obligations of the operator:	➢ The new version of the poker game engine is assimilated as a new component of the gaming software. It is therefore subject to approval before it is put into operation. ➢ The scope of the audits should include, at a minimum, the new version of the game engine, with particular attention to the compliance of the implementation of the rules of the game and game primitives.
Main requirements:	➢ Scope of application: **[E_HOM_CHA1], [E_HOM_CHA3]** ➢ Scope of the audit: **[E_HOM_PER3]** ➢ Poker Software: **[E_HOM_SEC1], [E_HOM_CFM1]**
Need for gaming software approval?	➢ YES
Contents of the approval application file	☑ The gaming software approval application form, provided; ☑ Functional description of the gaming software and its developments; ☑ Technical description of the gaming software and its developments; ☐ Functional description of the RNG and its developments; ☐ Technical description of the RNG and its developments; ☐ The justification for the technological choices implemented for the RNG; ☑ The gaming software security audit report; ☐ RNG quality and security audit report; ☑ The compliance audit report implementing the business rules; ☑ The gaming regulation displaying the rules of the game; ☑ The remediation plan; ☑ The source codes of the gaming software; ☐ Source codes of the RNG device.

Scenario No 5: bug fixes

Initial situation:	➢ The gaming operator has horserace betting software, which is already approved, composed of: ○ A game engine for managing bets, incorporating a totaliser for calculating the masses of stakes and ratios; ○ A web-based betting app (desktop and mobile sites); ○ API services relaying player requests, *via* the web-based betting app, to the game engine.
Description of the development:	➢ The gaming operator has made some bug fixes on its mobile site.
Obligations of the operator:	➢ Corrections to the gaming software, provided they do not alter the game mechanics, the rules of the game and their implementation, as well as the security mechanisms already in place, are considered minor changes. Therefore, they do not give rise to a new approval of the gaming software. ➢ In case of doubt as to the substantial nature of the changes made to the gaming software, consulting the ANJ is strongly recommended.
Requirements:	➢ Scope of application: **[E_HOM_CHA3]**
Need for approval?	➢ NO

Scenario No°6: minor changes

Initial situation:	➢ The gaming operator has approved online gaming software, composed of: ○ A game engine; ○ A web application available to gamers (gaming client); ○ API services relaying player requests, *via* the web application, to the game engine.
Description of the development:	➢ The gaming operator has updated the appearance of its online game site. Only the visual aspect of the site is changed (*i.e.* the colours, images, positioning and size of the interface elements, addition of a new section of news). ➢ The features of the gaming software have not been changed.
Obligations of the operator:	➢ The game mechanics, the rules of the game, the associated implementation and the security mechanisms of the gaming software remain unchanged. The changes made may be treated as minor changes. They do not give rise to a new approval of the gaming software.
Requirements:	➢ Scope of application: **[E_HOM_CHA3]**
Need for approval?	➢ NO

Scenario No 7: change of gaming solution provider

Initial situation:	➢ The gaming operator's poker offer is hosted on the gaming platform provided by a Provider A.
Description of the development:	➢ The gaming operator migrates its poker offer to the gaming platform of a new Provider B. ➢ Following the migration of the offer, Provider A's poker software, which is approved, will be left for Provider B's poker software (including thick clients, mobile applications and the RNG device). ➢ Provider B already provides its poker software to other licensed gambling operators. This poker software is already approved for these operators and has not undergone any substantial development since it was last granted approval.
Obligations of the operator:	➢ The approval of a gaming software is only valid for gaming operators who have made an express request to the ANJ services. ➢ As a result, Provider B's poker software (including RNG device) is not approved for operators who are migrating their poker offer and will be considered, by the Authority, as a new software that has not yet been approved. The operator will therefore have to submit, in its name, to the ANJ, an application for approval of the poker software of Provider B which it intends to operate in the course of its poker activity. ➢ Auditors will focus their attention on the security of the gaming software, gaming clients and RNG device. ➢ The conformity of the implementation of the business functions (rules of the game, game mechanics) has already been checked during the previous approvals requested and obtained by the other operators using this gaming software. Under the assumption it has not undergone any substantial development since it was last granted approval, the compliance of implementation of business functions audit is not required.
Main requirements:	➢ Scope of application: **[E_HOM_CHA1], [E_HOM_CHA6]** ➢ Scope of the audit: **[E_HOM_PER1], [E_HOM_PER2]** ➢ Poker Software: **[E_HOM_SEC1], [E_HOM_GNA1], [E_HOM_CFM1]**
Need for gaming software approval?	➢ YES
Contents of the approval application file	☑ The gaming software approval application form, provided; ☑ Functional description of the gaming software and its developments; ☑ Technical description of the gaming software and its developments; ☑ Functional description of the RNG and its developments; ☑ Technical description of the RNG and its developments; ☑ The justification for the technological choices implemented for the RNG; ☑ The gaming software security audit report; ☑ RNG quality and security audit report; ☐ The compliance audit report implementing the business rules; ☑ The gaming regulation displaying the rules of the game; ☑ The remediation plan; ☑ The source codes of the gaming software; ☑ Source codes of the RNG device.

Scenario No 8: RNG device update

Initial situation:	➢ The gaming operator, for its poker activity, has a RNG device, which is already approved.
Description of the development:	➢ The gaming operator has updated its RNG device associated with its poker gaming software, to improve its security. To do this, the old RNG algorithm has been replaced by an algorithm with features that would make the RNG device robust against certain new attacks that predict the sequence of values produced.
Obligations of the operator:	➢ The modifications made directly affect the safety of the RNG device, rendering obsolete the previous analyses carried out during the last approval of the device. This development of the RNG device will therefore be considered by the Authority as a substantial development of the gaming software. The new version of the RNG device will therefore need to be re-approved before it is put into production. ➢ Auditors will focus their attention on the quality and the security of the RNG device.
Main requirements:	➢ Scope of application: **[E_HOM_CHA3]** ➢ Scope of the audit: **[E_HOM_PER3]** ➢ Poker Software: **[E_HOM_GNA1]**
Need for gaming software approval?	➢ YES
Contents of the approval application file	☑ The gaming software approval application form, provided; ☐ Functional description of the gaming software and its developments; ☐ Technical description of the gaming software and its developments; ☑ Functional description of the RNG and its developments; ☑ Technical description of the RNG and its developments; ☑ The justification for the technological choices implemented for the RNG; ☐ The gaming software security audit report; ☑ RNG quality and security audit report; ☐ The compliance audit report implementing the business rules; ☐ The gaming regulation displaying the rules of the game; ☑ The remediation plan; ☐ The source codes of the gaming software; ☑ Source codes of the RNG device.

Scenario No 9: redesign of horserace betting software available on point-of-sale automatic terminals.

Initial situation:	➢ The gaming operator has horserace betting software for its exclusive rights betting offer, which is already approved, including: ○ A game engine for betting management, incorporating a totaliser for calculating the masses of stakes and ratios; ○ Software, installed on the automatic terminals, at a point of sale, intended for betting and payments; ○ API services relaying player requests from automatic terminals to the game engine.
Description of the development:	➢ As part of its project to modernise the automatic terminals available at the point of sale, the operator plans to replace the terminals with new terminals based on new equipment. On this new hardware, a new gaming software for betting and payments will also be deployed. ➢ The rules, the game mechanics and the game offer remain unchanged. ➢ The gaming platform integrating the game engine, the totaliser and API services, remains unchanged.
Obligations of the operator:	➢ As a new game medium and a new gaming software, the new gaming software is subject to approval. ➢ Auditors will focus their attention on the security of the new software, new hardware and communication channels linking the terminal software to the gaming platform. ➢ Auditors will also analyse the conformity of the implementation of the rules of the game and the game mechanics at the level of the new software that will be deployed on the new terminals.
Main requirements:	➢ Scope of application: **[E_HOM_CHA1], [E_HOM_CHA7]** ➢ Scope of the audit: **[E_HOM_PER3]** ➢ Horserace betting software: **[E_HOM_SEC1], [E_HOM_CFM1]**
Need for gaming software approval?	➢ YES
Contents of the approval application file	☑ The gaming software approval application form, provided; ☑ Functional description of the gaming software and its developments; ☑ Technical description of the gaming software and its developments; ☐ Functional description of the RNG and its developments; ☐ Technical description of the RNG and its developments; ☐ The justification for the technological choices implemented for the RNG; ☑ The gaming software security audit report; ☐ RNG quality and security audit report; ☑ The compliance audit report implementing the business rules; ☑ The gaming regulation displaying the rules of the game; ☑ The remediation plan; ☑ The source codes of the gaming software; ☐ Source codes of the RNG device.

Scenario No 10: new software for printing physical scratch cards.

Initial situation:	➢ The operator approached a specialised printer and hired their services to print a defined number of physical scratch cards.
Obligations of the operator:	➢ The ticket printing software is subject to software approval because it carries part of the game mechanics by introducing randomness when printing the tickets.
Main requirements:	➢ Scope of application: **[E_HOM_CHA1], [E_HOM_CHA8]**
Need for gaming software approval?	➢ YES
Contents of the approval application file	☑ The gaming software approval application form, provided; ☑ Description of the ticket generation procedure and ticket printing device; ☑ Description of the printer's qualification process; ☑ The presentation of the safety elements presented in the qualification file that led to the retention of the printer; ☑ The presentation of contractual clauses available to the gaming operator in respect of its printers, relating to the security of the printing device and its auditability; ☑ The audit reports carried out on printers regarding the printing software, the quality of the RNG on which the software relies to produce the tickets, and the means of securing the printing device.

VII.2 Annex 2 – Types of audit services expected

VII.2.1 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.

VII.2.2 Dynamic test

The purpose of a dynamic test service is to verify the presence of 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.

VII.2.3 Source code audit

The purpose of a source code audit service is to verify the presence of 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, analysis consists of validating the correct implementation of the security features and business functions related to the game mechanics and game rules displayed to users and of looking 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 include relevant source code extracts in the body of the 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 case of imposing source code, “directory” fingerprinting mechanisms may be provided. The fingerprinting mechanism should be clearly detailed and reproducible (see [E_HOM_AUD6]).

VII.2.4 Intrusive audit

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

VII.2.5 Differential intrusive audit

The differential intrusive audit associates the audit of the modified source code of the gaming software with an intrusion test.

The auditor will analyse changes to the gaming software since it was last approved to ensure that no security issues have been introduced. The methodology should be based on the methodology described in the intrusive audits.

VII.3 Annex 3 – 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.

VII.3.1 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 inherently 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.

VII.3.2 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.

VII.3.3 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 of the identified vulnerabilities depends on both the impact and ease of exploitation of the vulnerability and is determined based on the following matrix:

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

VII.4 Annex 4 – Safety and recommendations for use

Under the rules and recommendations set out in the General Security Standards (RGS) established by the National Agency for 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