ANJ

AUTORITÉ NATIONALE DES JEUX

FRENCH REPUBLIC

TECHNICAL REQUIREMENTS FOR THE GAMBLING OPERATORS' INFORMATION SYSTEMS

Summary

In accordance with Article 34(VIII) of the Law of 12 to Article 32 of Decree No 2010-518 in its version applicable from 1st October 2020, which provides that the Collège de l'ANJ (French Gambling Authority) determines the technical requirements necessary for its application, this document specifies the technical requirements for gambling operators information systems.

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

Table of Contents

I General description

I.1 Rappel des obligations légales et réglementaires

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

" The objective of the State's gambling 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 gambling 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 gambling to avoid any economic destabilisation of the sectors concerned."

Article L. 320-4 of the Internal Security Code:

" The gambling operators defined in Article L. 320-6 shall contribute to the objectives mentioned in 1., 2. and 3. of Article L. 320-3. Their gambling offer helps channel the demand for gambling in a circuit controlled by the public authority and prevent the development of an illegal gambling offer".

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

" The French Gambling Authority determines the technical characteristics of online gambling 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 gambling 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. [...]"

Decree of 27 March 2015 approving the specifications applicable to online gambling operators (Annex, Article 11).

I.2 Présentation du corpus des exigences techniques

In order to facilitate the readability and implementation of the different categories of technical requirements, the choice was made, on the one hand, to rewrite them in full in order to adapt the body of rules and to divide them into five volumes in order to facilitate their appropriation by gambling operators.

1. Volume 1: technical requirements for the licensing and security of information systems

This volume brings together the architectural and material obligations, as well as the organisational, informational and procedural obligations expected in relation to the security policy of information systems.

The objective here is to assess the technical and human resources used to manage the risks associated with technical and functional systems for data collection, management and storage.

These requirements shall be implemented by the operator as soon as the license is obtained and the presentation of their implementation underpins the technical part of the instruction of the application for renewal of the license. Without formal authorisation, the part of the information system for operators holding exclusive rights covering gambling covered by these exclusive rights must conceptually incorporate the same requirements, insofar as the requirements set out here relate to the entire information system or cross-functional components.

Dealing comprehensively with the information system and linked to the maturity of the organisation in terms of security, this volume takes on its full meaning only in conjunction with the other volumes.

2. Volume 2: technical requirements for software certification

This document sets out the framework for the approval of gambling and betting software to ensure the integrity and security of gaming software.

It defines the scope of approval, its technical perimeter and details of the procedure, formalising and structuring the documents and information expected from operators.

3. Volume 3: technical requirements for the provision of data pursuant to Articles 31 and 38 of Law No 2010-476 of 12 May 2010

This volume enables to define the mechanisms to be put in place in order to guarantee the integrity and consistency of the recording of gambling data, the procedures for making available and the formalism of the recordings made via the physical storage medium (PSM).

It also seeks to define the information that operators must provide at all times through the PSM in order to enable the Authority to carry out its task of constantly monitoring the activity of gambling operators (Articles 31 and 38 of Law No 2010-476 of 12 May 2010).

4. Volume 4: technical requirements for querying the gambling prohibition file

This volume defines the technical procedures (formation of query keys, channels and consultation mechanisms of DNS services) to be implemented by the operators in order to query the gambling prohibition file pursuant to Article 22 of Decree No 2010-518 of 19 May 2010 as amended.

This volume does not envisage the Authority's management of the file.

5. Volume 5: technical requirements for certification

This section includes all the technical requirements relating to the architecture and security measures to be examined by the certifying bodies in connection with the certification of the PSM, 6 months after the launch of the activity, and the annual certification provided for by the provisions of Article 23 of amended Law No 2010-476 of 12 May 2010 to ensure that an adequate level of system security is maintained.

Volumes 1 to 5 apply throughout an operator's activity.

I.3 Présentation et objectifs du document

In accordance with the provisions of Article 34(VIII) of Law No 2010-476 of 12 May 2010, as amended, on the opening up to competition and regulation of the online gambling sector, the ANJ establishes the technical characteristics of platforms and software for online gambling and betting of operators subject to a licensing regime and operators holders of exclusive rights.

To this end, this document sets out the technical requirements for the licence application which marks the entry of an operator on the market and then expires after 5 years when the licence is renewed. But the requirements must be understood as technical, security and organisational requirements which must necessarily be permanent for all operators.

The licensing procedure for gambling operators must enable the Authority to ensure:

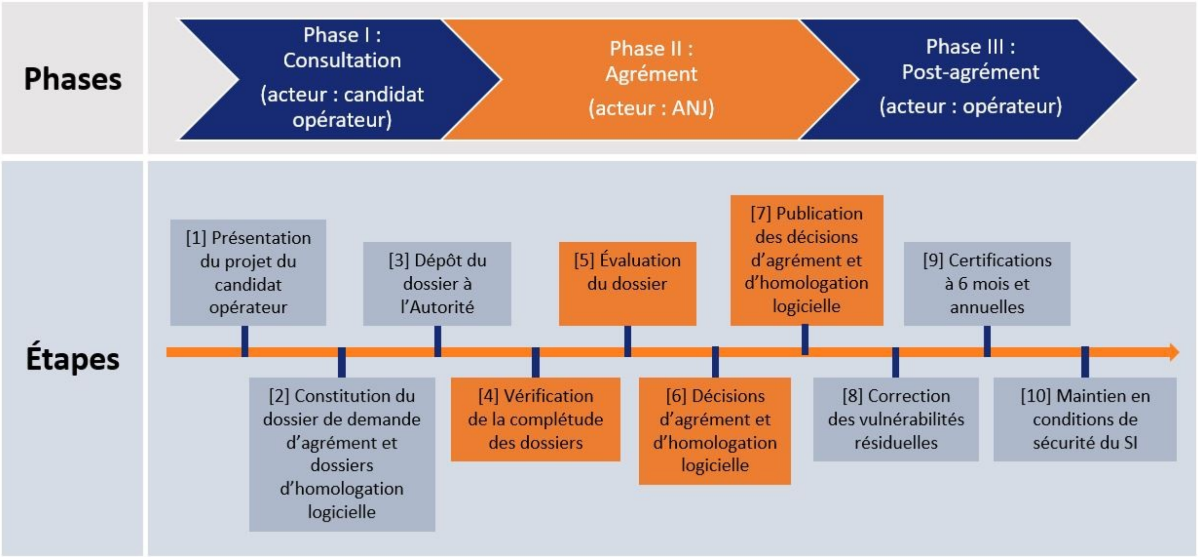
- compliance with PSM rules. In the case of a new operator for which the PSM would not yet be in place, the challenge is to ensure that its implementation strategy incorporates the PSM requirements;
- the long-term security and robustness of the information system, both in its technical and organisational components, on which the games and related services (player account services, payments, gambling operations, etc.) are implemented by the operator.

The actions taken by the Authority in this context form part of the control system it has put in place, aimed at meeting the objectives set out in Article L. 320-3 of the Internal Security Code. If the assessment of a license application shows that the resources implemented do not allow the fulfilment of these objectives, the ANJ will reject the license application. More specifically, it follows from the first subparagraph of Article 21(III) of the amended Law of 12 May 2010 that the Authority may refuse to issue or renew a license "*on grounds of the technical inability (…) of the applicant to sustainably meet the obligations attached to his activity or the safeguarding of public order, the fight against money laundering and the financing of terrorism, the requirements of public security and the fight against excessive or pathological gambling*".

The document presents:

- the scope of the licensing procedure, i.e. in which cases the operator must apply for a license (section II);
- the scope of the license on the IS component in its principles (section III);
- the content of the license file for the IS component, i.e. the documents composing it and the requirements for each of these documents in terms of the content and organisation of the information requested (section IV)
- the licensing procedure (section V);
- the follow-up to the license (section VI).

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


Phases
Phase I : Consultation (acteur : candidat opérateur)
Phase II : Agrément (acteur : ANJ)
Phase III : Post-agrément (acteur : opérateur)
Étapes
[1] Présentation du projet du candidat opérateur
[2] Constitution du dossier de demande d'agrément et dossiers d'homologation logicielle
[3] Dépôt du dossier à l'Autorité
[4] Vérification de la complétude des dossiers
[5] Évaluation du dossier
[6] Décisions d'agrément et d'homologation logicielle
[7] Publication des décisions d'agrément et d'homologation logicielle
[8] Correction des vulnérabilités résiduelles
[9] Certifications à 6 mois et annuelles
[10] Maintien en conditions de sécurité du SI

Phases	Phases
Étapes	Steps
Phase I : Consultation (acteur : candidat opérateur)	Phase I: Consultation (actor: applicant operator)
Phase II : Agrément (acteur : ANJ)	Phase II: License (actor: ANJ)
Phase III : Post-agrément (acteur : opérateur)	Phase III: Post-licensing (actor: operator)
[1] Présentation du projet du candidat opérateur	[1] Presentation of the applicant operator's project
[2] Constitution du dossier de demande d'agrément et dossiers d'homologation logicielle	[2] Constitution of the license application and software certification files
[3] Dépôt du dossier à l'Autorité	[3] Submission of the file to the Authority
[4] Vérification de la complétude des dossiers	[4] Verification of completeness of files
[5] Évaluation du dossier	[5] Evaluation of the file
[6] Décisions d'agrément et d'homologation logicielle	[6] Software approval and licensing decisions
[7] Publication des décisions d'agrément et	[7] Publication of software approval and

d'homologation logicielle	licensing decisions
[8] Correction des vulnérabilités résiduelles	[8] Correction of residual vulnerabilities
[9] Certifications à 6 mois et annuelles	[9] 6-month and annual certifications
[10] Maintien en conditions de sécurité du SI	[10] Maintaining the IS in secure conditions

I.4 Glossaire

This glossary covers all technical requirements for Volumes 1 to 5. Each volume reproduces identically the elements of the glossary with the sole objective of facilitating the work of the reader by allowing him to have a self-sufficient document.

GDPR: General Data Protection Regulation

Cloud: “cloud computing service”: a digital service that allows access to a flexible and variable set of IT resources that can be shared;

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

Cyber-risk: cyber-risk refers to any breach of computer and communication systems, as well as stored or transferred data. These incidents, likely to block the functioning of the organisation, can be caused by malicious acts, unintentional human errors or technical malfunctions.

Availability: the property of being accessible and usable on request by an authorised entity.

Incident management: all procedures relevant to the detection, analysis and containment of an incident and all procedures and protocols relevant to the incident response.

Incident: any event that has a real negative impact on the security of information systems and networks.

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: the operator’s computer system, dedicated to a gaming activity. This mainly consists of hardware and software resources that particularly ensure the complete management of gambling operations.

Risk: a combination of a threat and the losses that it may cause, i.e. the appropriateness of exploiting one or more vulnerabilities of one or more entities by a threatening element employing an attack method with the impact on the essential elements and on the organisation.

Residual risk: risk remaining after the risk management process.

IT system: an IT system represents all of the hardware and software resources organised to collect, store, process and communicate information.

Information System Security (ISS): the security of an information system involves reducing the risks to the information system, in order to limit their impact on the operation and business activities of companies.

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.

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 constituent element of the collection and archiving system, whose function is to create traces. The trace creation function corresponds to the formatting of the data circulating between the player and the gaming platform and then transferring this data to the vault module of the collection and archiving system.

Vault: a constituent element of the PSM, whose function is to encrypt, sign, time-stamp and archive the data traced and collected from the stream originating from the player or provided by the gaming platform. This is in order to guarantee confidentiality, authenticity and completeness over time.

Physical Storage Medium (PSM): a device for collecting and storing data exchanged between the player and the operator's gaming platform during gambling operations. This device shall be developed and operated under the responsibility of the operator.

ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information (National Cybersecurity Agency of France).

CNIL: Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority).

Security requirement: security property to be guaranteed for information, process, service or material asset (examples: availability, integrity, confidentiality).

Security directive: application of the ISSP to a specific theme.

Sensitive data: within the meaning of these requirements, sensitive data is unclassified information or material, which, if it were disclosed to the public (via any means of communication, to the professional circle without the need to know, or in the context of the personal environment) or if a document were falsified, could harm the image or interests of the ANJ, operators holding an authorisation or exclusive right, organisations bound by contract or agreement or their staff.

e.g.: audit reports (approval, certification, license, etc.), source codes, approval report, instruction reports, action plan, etc.

Sensitive document: a sensitive document is a document that must not be brought to the attention of people (including internally) who do not need to know it.

Dreaded event: an incident that affects the availability, integrity and/or confidentiality of information, process, service or material asset (e.g.: unavailability of the file server).

Severity: estimate of the level and intensity of the effects of a risk. Severity provides a measure of perceived adverse impacts, whether direct or indirect.

Security approval: validation by an approval authority that the level of security achieved by the organisation meets expectations and that the residual risks are accepted within the scope of the study.

Certification: analysis that enables a customer to ensure, through the intervention of a competent and controlled independent professional, called a certifying body, that a product complies with one or more standards.

Security incident: an event or a set of events that affects the availability, integrity and/or confidentiality of information, process, service or material asset.

Threat: a generic term for any hostile intent to cause harm.

Security measure: means of dealing with a risk in the form of solutions or requirements that can be included in a contract. A measure can be functional, technical or organisational. It can affect information, a process, a service, a material asset, a stakeholder in the ecosystem.

Stakeholder: a person, group of people, organisation or source of risk in direct or indirect interaction with the subject of study (examples: a service provider working on an IS system, a supplier).

Business Continuity Plan (BCP): a formalised set of procedures and measures designed to ensure that the business activity continues without interruption and to ensure the availability of information regardless of the incidents encountered.

Disaster Recovery Plan (DRP): a formalised set of procedures to be followed for the restoration and reactivation of an information system in the event of a disaster or major incident resulting in a business interruption (examples: fire, breakdown, etc.).

Information Systems Security Policy (ISSP): a formalised set of strategic elements, directives, procedures, codes of conduct, organisational and technical rules, with the aim of protecting the information system(s).

Security principle: the security principles are the expression of the necessary security guidelines and the important characteristics of the ISS for the development of an ISSP.

Sensitive position: a human resources position, which may have direct or indirect access to personal data within the meaning of the GDPR or gambling operations or sensitive data.

Security rule: security rules define the means and behaviours within the framework of the ISSP. They are created by applying security principles in a given environment and context.

Risk: scenario describing a dreaded event and all the threats that make it possible. Its level is estimated in terms of severity and likelihood.

Initial risk: risk scenario assessed prior to application of the risk treatment strategy. Its level is estimated in terms of severity and likelihood.

Residual risk: risk scenario remaining after application of the risk treatment strategy. Its level is estimated in terms of severity and likelihood.

Software as a Service (SaaS): a software business model in which a third party provider hosts software applications and makes them available to its customers through online services.

Source of risk: an element, a person, a group of people or an organisation likely to generate a risk, accidentally or deliberately.

Information system (IS): the 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.

The information system should not be confused with the IT system, which is only a subset of the former.

IT system: all the IT resources necessary for the processing of information (computers, programmes, network, software, etc.).

Likelihood: estimate of the probability of a risk occurring.

ANJ: Autorité Nationale des Jeux (French Gambling Authority).

Online gambling and betting: gambling and betting where the commitment is made through an online public communication service.

Rules of the game: a set of standards governing the conditions under which a game is played. The game 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 this document, it is understood as all calculations, processing of information and behaviours allowing the implementation of the rules of play defining the game.

Primitive (of the game): elementary game information processing function. The sequence of a coherent set of game primitives aims to create game mechanics.

Business functions (in the sense of gaming software): a set of game primitives and functions contributing to the implementation of game mechanics and rules defining a game.

Software architecture: organisation of the various components of a software package.

Information system (IS): a 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 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).

Gaming software: all the computer applications or programmes implementing the game mechanics.

Any computer application or programme 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;
- One or more game 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 services[1], 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 breakdown into business components described above, the software approval can be processed in a modular fashion.

Game engine: a component of the gaming software, usually integrated into the gaming platform, responsible for providing gaming primitives to the gaming software, or even ensuring the complete management of gambling operations (examples: taking bets in sports and horse racing, drawing and dealing 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 game rules and mechanics are usually driven by the game engine.

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

Game client: a component of the gaming software, made available to players or betters, or even point-of-sale retailers, enabling the latter to interact, in a “client-server” relationship, with the gaming platform, in particular the game engine (examples: consultation of the gambling offer displayed by the operator, placing of bets, consultation of betting results and associated winnings).

The game client can implement all or part of the game mechanics and come in various forms:

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

[1] API: Application Programming Interface. A 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 fat client to be installed on the user's workstation;
- Application for mobile devices or tablets;
- Application for point-of-sale terminals;
- Automatic remote gambling processing system (e.g.: software for betting via SMS or instant messaging).

It should be noted that the game client is conceptually distinct from the application client used. For example, in the case of a mobile phone application, the application client contains the game client but may also contain services such as account management, game statistics, news, etc. The approval of the game client is not intended to cover these ancillary services, but it is necessary to ensure that the game client is properly isolated in terms of security.

(Automatic) terminal, also known as gaming terminal without human intermediation: a hardware device, positioned in a physical distribution network (examples: racecourses, retailers, tobacconists), incorporating a gaming client-type software interface, directly accessible to players or betters. 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 (deposits and withdrawal of money) under conditions previously notified to the players.

Point-of-sale terminal, also known as gaming terminal with human intermediation: the point-of-sale terminal has the same functions as the point-of-sale station, however, access to the software interface is restricted to the personnel authorised by the operator and the point of sale managers (examples: retailers, tobacconists). The terminal can have management functions dedicated to retailers (stock management, accounting, ticket sales, etc.).

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

Random Number Generator (RNG): a 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 variable, for example, in poker with the random drawing of cards or even online lottery games without a physical draw.

I.5 Identification des exigences et recommandations dans le document

This document has two levels of recommendations:

- The measures preceded by **[E_numero]** are requirements that are **mandatory**, subject to the exceptions mentioned in these technical requirements;
- The measures preceded by **[R_numero]** are recommendations, which operators may decide not to follow, provided that they justify this to the Authority and inform it of the

alternative measures they intend to implement.

II Scope of application of the license

The following requirements refer to the cases in which a license is required:

[E_AGR_CHA1] A new operator is systematically approved before any software approval decision, which must precede any opening of a game offer.

[E_AGR_CHA2] An operator with a license must renew it at the end of its 5-year validity. The renewal procedure is strictly identical to the original procedure. The file submitted to the authority will specify what elements have changed from the situation 5 years earlier.

III Scope of the IS component of the license

[E_AGR_PER1] The scope of the IS component of the license covers all the organisational and technical aspects of the operator's IS as implemented (case of a renewal of license) or to be implemented (case of a new license), with a particular focus on the specific components related to gambling (player account, sensor, PSM, etc.) and the security of the IS as a whole.

IV Content of the license file for the IS component

IV.1 Liste des documents exigés et dispositions communes

[E_AGR_DOS2] The license application file of a gambling operator submitted to the ANJ, in a dematerialised format includes the following documents:

1. the information system master plan;
2. the information systems security policy;
3. a framework document describing a comprehensive and detailed architecture. This document will be accompanied by the following annexes:
   a. an attachment presenting the PSM (sensor and vault);
   b. an attachment presenting the player account management tool and player access channels;
   c. an attachment presenting IS platforms and supplier tools;
   d. an attachment setting out the processes and level of service (SLA);

The provisions relating to each of the documents listed above, and in particular the expected content, are detailed in the following sections.

[E_AGR_DOS2] Except for a new operator who has not yet fully implemented the infrastructure and processes, the different documents must reflect the current situation at the time of filing, in particular the ISSP and master plan must correspond to the current version.

The attention of the operator is drawn to the fact that the failure to comply with this obligation **[E_AGR_DOS2]** is a ground for refusal of the license application.

[E_AGR_DOS3] In the event that certain sections of the documents present only the forecast, without the work being finalised, by a new operator who has not yet put in place all its infrastructure and processes, it must:

1. include the timetable for completing these in the license application file;
2. communicate the additional information to the Authority in accordance with the timetable communicated;
3. and submit these elements to the certifier for analysis at the next certification.

This, provided that the absences in question do not constitute an incompleteness of the file that hinders its examination, which is a matter for the Authority to assess.

IV.2 Dispositions relatives au schéma directeur du système d'information

[E_AGR_DIR1] The information system master plan will follow the detailed plan below:

1. Corporate strategy at 3-5 years;
2. information system strategy;
3. organisation of the information system function;
4. human resources of the information system function;
5. budgetary resources;
6. IS governance.

The document may contain additional sections if the operator or auditor deems it necessary.

In the event that applicable documents correspond to the content requested for the above-mentioned chapters, then a correspondence matrix between the plan described above and the specific sections and pagination of the document(s) shall be provided by the licensing candidate.

[E_AGR_DIR2] The "corporate strategy" chapter describes the following:

1. The date of preparation of the master plan, the period covered and the planned update dates shall be specified.
2. the company's strategy over a 3 to 5 year time scale presenting its context, ambition and positioning;
3. business challenges associated with this target.

[E_AGR_DIR3] The "information system strategy" chapter describes the following:

1. IT guidelines covering the entire scope of the IS;
2. structuring IS projects responding to business challenges, their detailed objective, possible phasing and their timetable. The ISS component in each project should be explained.
3. For projects launched, a summary of the progress to date is attached.

[E_AGR_DIR4] The "organisation of the information system function" chapter contains, at least, the following:

1. the different structures that compose it, with their specific missions;
2. any related entities, with their respective functions and geographical locations;

[E_AGR_DIR5] The "human resources of the information system function" chapter contains, at least, the following:

1. the corresponding number of internal staff and full-time equivalent (FTE) by structures and missions of the information system function are specified, distinguishing at least between the functions of operation, information system security, infrastructure projects, application projects & MCO, management & strategy;
2. where appropriate, changes in staff forecast over the time scale of the master plan;
3. the outsourcing policy applicable to the information system function;
4. it specifies the businesses or functions involving subcontracting or outsourcing (in particular web hosting, facilities management, security, etc.) and the corresponding volumes (FTE).

[E_AGR_DIR6] The "Budgetary resources" chapter contains, at least, the following:

1. the overall annual forecast IS budget over the time scale of the master plan;
2. its estimated distribution by major areas (operational function, information system security, infrastructure projects, application projects & MCO), by year over the period covered by the master plan;
3. its projected annual distribution over the time scale of the master plan by structuring IS projects that reflect the IS strategy.

[E_AGR_DIR7] The "IS governance" chapter describes the following:

1. The players involved in IS governance, their respective roles and responsibilities.
2. The comitology set up for the management of the IS projects portfolio, including in particular the structuring projects mentioned in the "information system strategy" chapter.

IV.3 Dispositions relatives au document décrivant la politique de sécurité des systèmes d'information

[E_AGR_SSI1] The Information Systems Security Policy (ISSP) follows the detailed plan below:

1. Policy, organisation, governance;
2. Human resources;
3. Asset management;
4. Integration of the security of information systems into the life cycle of projects;
5. Physical security;
6. Network security;
7. Architecture of information systems;
8. Operation of information systems;
9. Security of the workstation;
10. Security of systems development;
11. Handling of incidents;
12. Business continuity;
13. Compliance, audit, control

The document may contain additional sections if the operator or auditor deems it necessary.

In the event that applicable documents correspond to the content requested for the above-mentioned chapters, then a correspondence matrix between the plan described above and the specific sections and pagination of the document(s) shall be provided by the licensing candidate.

[E_AGR_SSI2] Detailed technical breakdowns of the elements required by its security policy are provided with their link to the ISSP, including the procedures related to information systems as well as the means (organisational and technical) of ensuring security and their monitoring over time.

[E_AGR_SSI3] The "Policy, organisation, governance" chapter describes:

- The start date of application of the information systems security policy;
- The periodicity of updating the information systems security policy;
- The strategic orientations and the level of implementation of the resulting actions;
- The scope of application of the information systems security policy;
- The legal and regulatory aspects related to the scope of application of the security policy;
- The scale of requirements, which shall include a weighting and reference values in accordance with the security criteria chosen and a list of impacts backed up by examples;
- A description of the security requirements of the operator's areas of activity, in accordance with the scale of requirements presented in the previous section;
- Analysis of the threats selected and not selected for the scope of the study, with justifications;
- A description of the organisation set up to ensure the security of information systems and the physical security of the premises;
  The existence of the following functions and the information requested shall be indicated:
  - Information system security officer: precise definition of responsibilities, degree of formalisation, number of assistants and reporting line;
  - Information system (IS) operating authority (or equivalent function): precise definition of responsibilities, degree of formalisation and, where applicable, nature of information systems security (ISS) responsibilities;
  - Specialist ISS lawyer: number and reporting line;
  - Internal ISS auditors: number and reporting line;
  - ISS internal control function: number and reporting line;
  - ISS support function: number and reporting line;
  - ISS operational function: number and reporting line);
  - ISS design function: number and reporting line;
- ISS dashboard models;

[E_AGR_SSI4] The "Human Resources" chapter describes the proportion of the operator's staff who have been sensitised or trained in the ISS in the IS and ISS chains and among users. It also specifies whether there is regular management and monitoring of everyone's competence.

[E_AGR_SSI5] The "Asset management" chapter describes the procedures and mechanisms put in place to protect the data processed by the operator, in particular:

- Personal data of its customers;
- Data and statistics relating to the game or certain players, knowledge of which could give a player an advantage;

- “Secret" game data (for example other players' cards or cards that have not been turned over in a poker game).
- The procedures for identifying and classifying sensitive components (including data) and the related methodology;

[E_AGR_SSI6] The “Integration of ISS into the project life cycle” chapter describes:

- The security management implemented by the operator at each stage of the system development cycle, in the definition, development, operation and use phases, then maintenance and development. The operator shall set out its policy in the event of an identified vulnerability and the absence of remedial provisions;
- The ISS acceptance procedure for information systems projects before they are put into service and specifying the proportion of information systems which have actually been the subject of such an acceptance;
- The procedures for implementing any formalised examination of the impact on IS security or the commissioning of a new component (server model, operating system, application, data, etc.) ;
- Risk studies carried out. The methodology is specified;
- Controls carried out on subcontractors to ensure that the level of security of its platforms and information systems is maintained.

[E_AGR_SSI7] The “Physical security” chapter describes:

- The procedures for verifying candidates applying for a sensitive position;
- Procedures for managing conflicts of interest;
- Procedures for safeguarding information when employees leave the company;
- Security measures for its staff;
- The means used to protect technical premises;
- Fire protection measures implemented;
- The power supply redundancy policy;
- The H24 monitoring policy of its operating sites;
- Physical access management policy;

[E_AGR_SSI8] The “Network security” chapter describes:

1. Computer and network operations and supervision centres: their location, hosted applications and staff assigned;
2. Hosting centres: their location and type of hosting;
3. Interconnection centres: the types of interconnections used;
4. Operational centres;
    a. For gaming platforms, front-end, and all related information systems, the license applicant shall specify:
    b. The function(s) performed;
    c. The type of data processed;
    d. The company or authority responsible for its operation;
    e. The access provider;
    f. The hosting service provider.

5. The network partitioning applied
6. The network filtering policy and the description of the filtering rules in terms of white lists.
7. The types of network partitioning used (IP filtering, application filtering, VLAN, 802. 1X, NAP/NAC, etc.).
8. The security mechanisms implemented to defend against conventional IP attacks and associated protocols, in particular in relation to network denial-of-service attacks;
9. The technical and organisational measures taken in terms of the network resilience of its information systems, in particular with regard to combating denial-of-service attacks (distributed or otherwise, by exhausting bandwidth, or system resources) at the level of gaming platforms and the front-end: The operator describes in particular the technical processes implemented (load balancing, DNS TTL adjustment, dynamic IP re-addressing of platforms, and front-end) and associated organisational measures (alerting in case of attack, memorandum of understanding with ISPs to combat DDOS, etc.).

[E_AGR_SSI9] The "IS Architecture" chapter describes all the mechanisms and measures implemented to ensure the confidentiality and integrity of flows within its gaming platforms and front-end: these flows concern administrators who are part of the operator's staff such as operators, external administrators such as those who carry out remote maintenance of equipment, etc.

[E_AGR_SSI10] The "Operation of IS" describes:

1. Player identification and authentication mechanisms;
2. Players' access control mechanisms: details of any player profiles and rights partitioning mechanisms;
3. Cryptographic processes to ensure the authentication of components, confidentiality and authenticity of the following communications:
    a. Communications between the operator and the ANJ;
    b. Network communications between players and the operator;
    c. Network communications between modules within the front-end;
4. A description of all mechanisms and measures implemented to ensure the confidentiality and integrity of flows within its gaming platforms and front-end: these flows concern administrators who are part of the operator's staff, such as operators, external administrators such as those who carry out remote maintenance of equipment, etc.;
5. A description of the mechanisms for accessing the administration functions of the gaming platform and the front-end, including;
6. The measures implemented to ensure a high level of security in the management of authentication secrets (in particular, robust passwords, periodic changes, strong authentication) for the operator's operating staff;
7. The process of applying patches, and in particular in the event of a regression;
8. The technical procedures for going back in the event that a patch would cause a possible regression;
9. Description of the logging of alerts and how long they are stored.

[E_AGR_SSI11] The " Security of the workstation" chapter describes:

1. The supply procedure and workstation management policy;
2. The formalised procedure for configuring workstations;
3. Physical protection mechanisms against theft;

4. Managing privileges on workstations;
5. Managing roaming access such as teleworking;
6. Managing removable storage media.

[E_AGR_SSI12] The "Security of systems development" chapter describes:

1. The means that the operator uses to protect the personal data and privacy of players;
2. Control measures and methods for evaluating developments at each stage of a development project;
3. The secure development framework for projects for which the operator is responsible for the development;

The operator will communicate the contracts concluded with its service providers relating to the implementation of a secure development framework for the projects which it outsources.

[E_AGR_SSI13] The "Handling of incidents" chapter describes:

1. The operating mode of the operational centre responsible for the operator's ISS. It shall specify, in particular, the reporting, the standby system and the permanent staff. Failing this, it shall specify the procedures for monitoring and triggering alerts;
2. Procedures put in place to deal with incidents and fraud detection. It shall specify the level of dissemination of these documents and the alert procedures provided for.
3. The status of any ISS incidents or frauds that the operator could have noticed. It shall specify the occurrences (in particular the identification of sources of entry and level) and the management that has been carried out;
4. The solutions implemented to prevent or detect, where appropriate, attacks and intrusions on its information systems.

[E_AGR_SSI14] The "Business continuity" chapter describes:

1. The archiving service with a view to ensuring the storage of all its processing data, and in particular that stored in the front-end vault. The operator specifies the type of media and the backup format,
2. The archiving mechanisms and the secure means of protecting the archives that the operator is capable of implementing;
3. The terms of its back-up plan. The operator shall specify in particular the procedures and deadlines for restoring a backup following an incident as well as the location(s) where the backups are stored and the security measures applied to the location(s).
4. The business continuity plans and the disaster recovery plans that the operator has been able to draw up as part of its business and the procedures it provides for adapting them to the front-end context.

[E_AGR_SSI15] The "Compliance, audit, inspection, control" chapter describes the nature, periodicity, actors and methodology of ISS audits carried out on information systems and applications. The operator communicates the reports and the main recommendations. It shall specify how corrective measures are to be decided, implemented and monitored. It shall state the proportion of measures actually applied.

IV.4 Dispositions relatives au document chapeau décrivant l'architecture globale et détaillée

[E_AGR_ARC1] the document describing the overall and detailed architecture of the IS will follow the detailed plan below:

1. The general description of the information system platform:
    a. All components implemented in the IS and, for each, the function(s) it performs;
    b. The type of hosting of each component;
    c. All the interconnections between components and, for each, a description of its purpose so that it is defined how the components work together to ensure the overall functioning of the system;
    d. The company or authority responsible for the operation of each component.
    e. Computer and network operations and supervision centres, specifying their location(s), operating methods and an estimate of the number of FTEs implemented;
    f. Hosting centres (location, type of hosting);
    g. Interconnection centres (types, suppliers);
    h. Operational centres (including security centre, customer service centre, development service centre, etc.);
    i. Network access providers for each outgoing/incoming IS link;
    j. It will also specify the list of the main software applications implemented in the context of the activities related to the licenses or activities concerned.
2. The overall presentation of the architecture with logical and physical network diagrams, application diagrams, network mapping;
3. The provisions relating to the attachment presenting the PSM (see chapter below);
4. The provisions relating to the attachment presenting the player account management tool and player access channels (see chapter below);
5. The provisions relating to the attachment presenting IS platforms and supplier tools (see chapter below).

The document may contain additional sections if the operator or auditor deems it necessary.

In the event that applicable documents correspond to the content requested for the above-mentioned chapters, then a correspondence matrix between the plan described above and the specific sections and pagination of the document(s) shall be provided by the licensing candidate.

IV.5 Dispositions relatives au document annexe présentant le SMA

[E_AGR_SMA1] At the time of submission of the license application file, the PSM is not necessarily in operation. However, the company must be able to present its detailed implementation strategy planned for it for the collection and backup of all the data it is used to collect.

[E_AGR_SMA2] To do this, the company provides a document describing the PSM. This document will follow the plan detailed below and may contain additional sections if the company deems it necessary:

1. General description of the PSM;

2. Detailed description of the sensor for trace generation;
3. Detailed description of the vault for secure storage of traces;
4. Description of the trace access functions collected by the PSM;
5. Special provisions relating to the front-end of the gaming platform;
6. Technical annexes.

The document may contain additional sections if the operator or auditor deems it necessary.

In the event that applicable documents correspond to the content requested for the above-mentioned chapters, then a correspondence matrix between the plan described above and the specific sections and pagination of the document(s) shall be provided by the licensing candidate.

[E_AGR_SMA3] The "General description of the PSM (vault and sensor)" chapter contains the following sections:

1. The overall strategy employed: this involves presenting the general operation implemented or envisaged, with regard to the secure collection and storage of traces;

2. The general architecture, presenting the various components of the PSM, their role, their positioning in relation to the gaming platform and their interactions with the gaming platform, players and any other possible IS;

[E_AGR_SMA4] The "Detailed description of the **sensor**" chapter contains the following sections:

Overall framework:

1. The detailed strategy used for the sensor, relating to the generation of traces. This involves presenting the selected sensor solution and the associated operation vis-à-vis the exchanged data whose traces are required (example: choice of a sensor that cuts off the application flow between the player and the gaming platform for queries made by the player);

2. The strategy used with regard to the very high availability requested, specifying the measures implemented in the event of unavailability or malfunction of the sensor;

3. The risk analysis carried out on the sensor;

4. The applicable security policy, including a detailed description of the sensor security measures;

5. The sensor in the logical sense can consist of several physical sensors, potentially of different types. The requested description must be provided for each type of physical sensor implemented.

Implementation:

6. The identity and contact details of the service provider(s) responsible for the development and maintenance of the sensor or supplier of the selected sensor solution;

7. The detailed specifications of the sensor including:

a) The detailed functional and technical architecture (application and network) of the sensor;

b) The specifications of the interfaces and, where applicable, of the “proxy” functions (application flow) implemented by the sensor;

c) The description of the different flows (i.e. data type, protocols) passing through the sensor;

d) A detailed description of the mechanisms implemented for the (positive or negative) acknowledgement of traces by the gaming platform and the vault;

e) A detailed description of the mechanisms implemented for batch processing of traces, as regards the communication of traces to the vault;

f) A detailed description of the authentication and confidentiality mechanisms put in place in the context of data exchanges:

   - Between the player and the sensor;
   - Between the sensor and the gaming platform;

8. When the PSM is already implemented, the list and results of the audit tests carried out;

Hosting:

9. The physical location of the sensor;
10. How the sensor is hosted;
11. The identity and contact details of the service provider hosting the sensor;
12. The production of the hosting contract(s);
13. Documents relating to the administration and operation of the sensor;
14. The procedures implemented in particular in terms of protection against unauthorised access;

[E_AGR_SMA5] The "Detailed description of the **vault**” chapter contains the following sections:

Overall framework:

1. The detailed strategy employed for secure storage of traces. This involves presenting the vault solution retained and the associated operation;
2. The strategy used with regard to the very high availability requested, specifying the measures implemented in the event of unavailability of the vault;
3. The risk analysis carried out on the vault;
4. The applicable security policy, including a detailed description of the vault security measures;

Implementation:

5. The identity and contact details of the service provider(s) responsible for the development and maintenance of the vault or supplier of the selected vault solution;

6. The detailed specifications of the vault, including:

   a) The detailed functional and technical architecture of the vault;

   b) A detailed description of the authentication and confidentiality mechanisms put in place for the exchange of data:

      - Between the sensor and the vault;

      - Between the vault and the ANJ information system;

   c) Description of the various algorithms used for secure storage of traces (example: trace chaining);

7. When the PSM is already implemented, the list and results of the reports of tests carried out;

Hosting:

8. The physical location of the vault (this must be hosted in metropolitan France in accordance with Article 31 of Law No 2010-476 of 12 May 2010);

9. How the vault is hosted;

10. The identity and contact details of the service provider hosting the vault;

11. The production of the hosting contract(s);

12. Documents relating to the administration and operation of the vault, in particular:

    a) The precise specification of the planned ceremony of initialisation of the vault and the handing over of the necessary keys;

    b) The specification and role of the key pairs used;

    c) The detailed description of the mechanisms for the authentication of natural persons to access the vault;

    d) A detailed description of the administration and management functions of the vault's users;

13. The procedures implemented in particular in terms of protection against unauthorised access;

[E_AGR_SMA6] The "Description of trace access functions collected by the PSM" chapter contains the following sections:

1. A detailed description of the tool for remote consultation and collection of trace files, including:

   a) Detailed functional and technical specifications;

   b) When the PSM is already implemented, the reports of the tests carried out;

2. A detailed description of the tool for validating and extracting trace files, including:

    a) Detailed functional and technical specifications;

    b) When the PSM is already implemented, the reports of the tests carried out;

[E_AGR_SMA7] The "Technical Annexes" chapter contains:

1. When the PSM is already implemented:

    a) The source code of the sensor;

    The Authority reserves the right to request further, at the time of the examination of the license or subsequently:

    b) The source code of the vault;

    c) The source code of the tool for remote consultation and collection of trace files;

    d) The source code of the tool for validating and extracting trace files;

2. A copy of the minimum first-level security certification (CSPN) of the PSM vault (or the timetable for obtaining it, together with a note from the assessment centre or certification centre certifying that the certification procedure has been initiated);

    a) The CSPN will have to take into account at least the following elements in terms of threats:

        1. The submission or injection of unauthorised records;

        2. Alteration of records;

        3. Data theft;

        4. Denial of service;

    b) The CSPN must take into account at least the following elements, at the level of security functions:

        1. Strong authentication of users and administrators;

        2. The encryption, signature and time-stamping of events;

        3. The chaining of events.

[E_AGR_SMA8] Before starting its activity, the licensed operator shall declare to the ANJ that its PSM is in operating mode.

IV.6 Dispositions relatives au document annexe présentant la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs

[E_AGR_GCC1] the document describes the player account management tool and access channels offered to players will follow the detailed plan below:

1. Technical conditions for accessing and registering at the site for any player;

2. Technical means of ascertaining the identity of each new player, his age, his address and the identification of the payment account to which his assets are transferred;
3. Technical arrangements for collecting and paying bets and winnings from its website;

The document may contain additional sections if the operator or auditor deems it necessary.

In the event that applicable documents correspond to the content requested for the above-mentioned chapters, then a correspondence matrix between the plan described above and the specific sections and pagination of the document(s) shall be provided by the licensing candidate.

[E_AGR_GCC2] The applicant shall justify obtaining at least one top-level domain name with the ".fr" ending by producing a registration certificate. It shall declare, where applicable, all other top-level domain names with the ".fr" ending which it intends to use for access to its online gaming site and shall provide the documents justifying the corresponding registrations.

[E_AGR_GCC3] The applicant shall specify the following characteristics of his website:

1. Site map;
2. Trademarks;
3. Technical characteristics of the website, domain name;

The "Special provisions relating to the front-end of the gaming platform" chapter contains the following sections:

1. The detailed description of the ".fr" website set up:
   a. Host;
   b. Location;
   c. Source code;
   d. Security policy;
   e. Risk analysis;
   f. Administration, operation and security procedures in place;
2. The detailed description of the player connection redirection functions;

[E_AGR_GCC4] The applicant shall specify the game channels planned, which will enable customers to play: fat clients, native applications on smartphones or redirected to a website. The applicant will specify whether the website offers game functions. He will specify the planned timetable for opening these different channels.

IV.7 Dispositions relatives au document annexe présentant les plateformes SI et briques fournisseurs

[E_AGR_PLA1] the appendix describing the Company's IS platform will follow, for each of the components identified as part of the requirement **[E_AGR_ARC1]** described in paragraph IV.3 ***Provisions relating to the framework document describing the comprehensive and detailed***

architecture, the plan detailed below. It may contain additional sections if the operator or auditor deems it necessary:

1. A detailed architecture description of each of the IS components listed in the framework document in accordance with the requirement **[E_AGR_ARC1]**;
2. A detailed description of the network architecture and associated flows.

The document may contain additional sections if the operator or auditor deems it necessary.

In the event that applicable documents correspond to the content requested for the above-mentioned chapters, a correspondence matrix between the plan described above and the specific sections and pagination of the document(s) shall be provided by the licensing candidate.

[E_AGR_PLA2] For each section, the description shall specify:

1. components or parts of components which are subcontracted to external suppliers (this also applies if the entire platform is subcontracted);
2. The reasons for this subcontracting will be systematically stated;
3. the contractual agreements governing these subcontracts will be described, and in particular the commitments relating to service level, responsibilities and security.

[E_AGR_PLA3] For each of the sections, software tools or infrastructure elements that are under construction or not yet operational will be taken into account in the same way as components already in production, as if they were already in production for the scope implemented for the licenses or activities concerned.

[E_AGR_PLA4] The “detailed architecture description” chapters, written for each of the components listed, describe:

1. The detailed description of the component, highlighting each of its physical and logical constituents with for each:
   a. the function(s) performed;
   b. the type of data processed;
   c. the designated company or operating authority;
   d. where applicable, the encryption methods implemented;
   e. the importance of its function (from "work facilitation tool" to "essential tool"),
   f. the importance of its availability (from "no effect" to "blocking effect" in the event of total or partial system shut-down),
   g. the importance of data integrity (from “no effect” to “blocking effect” in the event of data modification);
   h. the importance of data confidentiality (from "no effect" to "blocking effect" in the event of data disclosure);
   i. the expected lifespan.
2. a detailed technical description of the network, in which the segmentation and filtering elements will be specified. Descriptions of the operational networks, but also those of the networks supporting administration and supervision.
   a. a technical diagram of the network;
   b. the list of the different associated flows;
   c. the list of areas with different sensitivities

   i. Typology (Internet or dedicated network, etc.)
   ii. Sensitivity;

d. the descriptive list of interconnections of these areas (role and purpose);
e. all the technologies implemented will be listed;
f. the list of external links (dedicated lines, network interconnections, etc.) and the remote access possible from the outside with for each a precise description of the technologies, protocols and security measures implemented.

IV.8 Dispositions relatives au document annexe présentant les processus et niveaux de service (SLA)

[E_AGR_PRO1] The appendix presenting the service processes and levels will follow the plan in two following chapters:

1. Administration and operating procedures
2. Service Levels (SLA)

The document may contain additional sections if the operator or auditor deems it necessary.

In the event that applicable documents correspond to the content requested for the above-mentioned chapters, then a correspondence matrix between the plan described above and the specific sections and pagination of the document(s) shall be provided by the licensing candidate.

[E_AGR_PRO2] The "administration and operating procedures" chapter describes the following:

3. the list of operating procedures used, which will be structured by theme. The security theme will need to be clearly explained. It should cover in particular:
   a. Log management procedures;
   b. Alert management procedures;
   c. Procedures for regular updating of all components (operating systems, applications, routers, etc.) ;
   d. Procedures for the management of components that require frequent updating (anti-virus, intrusion detection systems, where applicable);
   e. Update procedures in the event of a critical security patch being issued,
   f. Procedures for securing systems in the event of an emergency or imminent danger;
   g. IS components operating procedures (servers, routers);
   h. Account and password operating procedures;
   i. Procedures for managing the managed components;
   j. Physical security procedures (guarding, etc.) ;
   k. Backup and restore management procedures,
   l. Procedures in the event of a security incident;
   m. Remote administration procedures;
   n. Business continuity and recovery procedures (DRP and BCP).
4. documentation describing the procedures listed above will be provided. In order to facilitate the analysis, the list above will include the precise reference (document, section, page) of each procedure in the documentation.

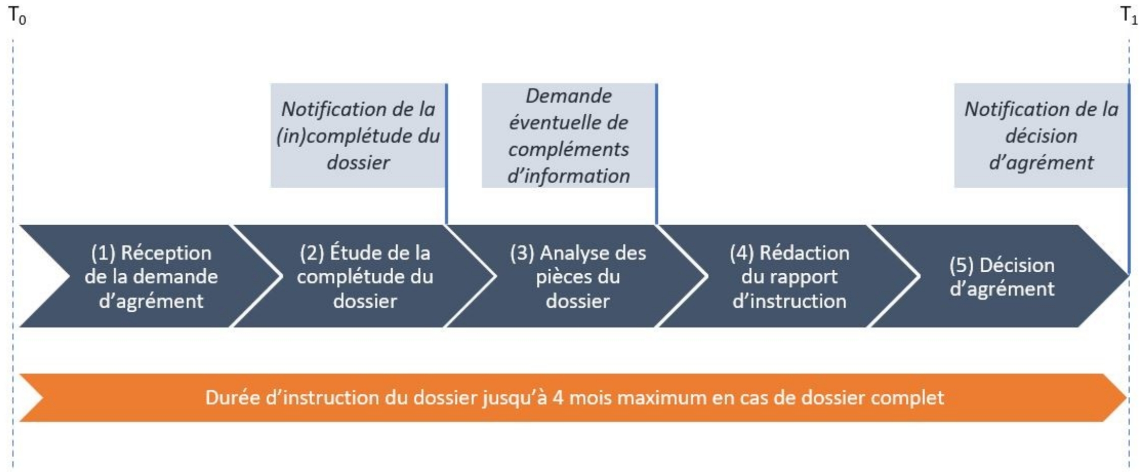
[E_AGR_PRO3] The "service levels and SLA" chapter describes the following:

1. The list of service levels (SLA) implemented both internally and externally with suppliers, classified by type (network, security, application availability, etc.).
2. For each SLA, the list shall specify the description of the indicator, the calculation method, its threshold(s), its internal or external character, the maximum time limit for intervention in the event of non-compliance.

IV.9 Dispositions relatives au formulaire du volet SI de l'agrément rempli

V Procedure for the licensing of a gambling operator

The diagram below presents the different stages in the license application assessment.



T_0
T_1
Notification de la (in)complétude du dossier
Demande éventuelle de compléments d'information
Notification de la décision d'agrément
(1) Réception de la demande d'agrément
(2) Étude de la complétude du dossier
(3) Analyse des pièces du dossier
(4) Rédaction du rapport d'instruction
(5) Décision d'agrément
Durée d'instruction du dossier jusqu'à 4 mois maximum en cas de dossier complet

Notification de la (in)complétude du dossier	Notification of (in)complete file
Demande éventuelle de compléments d'information	Possible request for additional information
Notification de la décision d'agrément	Notification of the licensing decision
(1) Réception t de la demande d'agrément	(1) Receipt t of the license application
(2) Étude de la complétude du dossier	(2) Study of the completeness of the file
(3) Analyse des pièces du dossier	(3) Analysis of the documents in the file
(4) Rédaction du rapport d'instruction	(4) Drafting of the evaluation report
(5) Décision d'agrément	(5) Licensing decision
Durée d'instruction du dossier jusqu'à 4 mois maximum en cas de dossier complet	Examination of the file up to a maximum of 4 months for complete files

V.1 Contenu du dossier

The license application file for a gambling operator submitted to the ANJ, in a dematerialised format includes the documents defined in the requirement **[E_AGR_PER2]** (see IV).

[E_AGR_PDA1] It is up to the gambling 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 examination of the application.

[E_AGR_PDA2] The absence of a document required in a license application file must be duly justified. Otherwise, the file will be considered incomplete.

[R_AGR_PDA3] In case of doubt, it is recommended to consult the ANJ before submitting any license application in order to avoid the suspension of the examination of the file, for reasons of incompleteness of the file in particular.

V.2 Modalités de transmission des livrables

[E_AGR_TRF1] The license application file must be submitted to the ANJ through the secure exchange channel made available to license applicants. A preliminary exchange is required to do this where the applicant will specify the surnames, first names and emails of its agents authorised to submit all or part of the file.

In the case of the PSM, when it is already in place, sending the source codes on a physical medium such as a USB key remains possible exceptionally, in which case the source codes will have to be encrypted and transmitted in accordance with the procedure that the ANJ has indicated to the operator.

V.3 Instruction de la demande

The ANJ has 2 months to consider the license application.

When the application for authorisation is made by an online gambling or betting operator, if the ANJ remains silent for 4 months on this application, this will be deemed to be a rejection decision (Article 8 of Decree No 2010-482 of 12 May 2010 as amended)

If the application file is not complete, the French Gambling Authority shall send the applicant company a letter asking it to remedy the situation within a period of not less than 15 days. The investigation shall be suspended during this period. If, by the expiry of the time limit, the requested information or documents have not been received by the Authority, the license application shall be rejected.
During the course of the investigation, the applicant company is required to provide, at the request of the French Gambling Authority, any information which is legally justified and that may enlighten the latter on the elements contained in the file submitted.

Licensing decisions are notified to the operator and published on the ANJ website.

VI Licensing scheme

VI.1 Cycle de vie

[E_AGR_SUA1] The newly licensed gambling operator will be required to submit a certification file at 6 months of the PSM upon initial implementation, in accordance with technical requirements volumes 3 and 5.

[E_AGR_SUA2] The licensed operator must, for any game it wishes to offer, submit a software approval file, in accordance with the technical requirements volume 2 and obtain a favourable decision before the service is provided to the players.

[E_AGR_SUA3] The licensed operator must open a gambling service no later than 1 year after obtaining the license, unless expressly agreed otherwise with the Authority.

[E_AGR_SUA4] the licensed operator shall ensure and maintain the security and robustness of its information system in all its components, in accordance with the technical requirements as a whole.

The operator is therefore expected to implement all the measures to meet this objective, in terms of technical updates, organisational structures and processes and appropriate control mechanisms.

[E_AGR_SUA5] Each year, on the anniversary of its licensing, the licensed operator must submit to the Authority a certification file in accordance with the technical requirements volume 5.

VII ANNEXES

VII.1 Article 12 renouvellement d'agrément

12.2.2. Information on the architecture of the information system.

The applicant shall provide ARJEL with the following elements:

a) An up-to-date description of the elements relating to the general presentation of the company and its information systems, as provided for in Article 11.4 of these specifications, in terms of:

-policy and organisation of information systems (11.4.1);

-description of information systems (11.4.2);

-human resources dedicated to IT security (11.4.3);

-piloting of information systems (11.4.4);

b) The file of definitions provided for in Article 11.5.2.1. of these specifications and in Article 5.7.3(a) of the Technical Requirements File (TRF);

c) An ANSSI attestation that the vault has been the subject of a maintenance report, as part of the first-level security certification assurance continuity procedure (CSPN), or a CSPN revaluation;

d) The vulnerability analysis report of the platform provided for in Article 11.3.2 of these specifications, consisting of an "intrusive audit" type report, the purpose of which is to search for and exploit the vulnerabilities of a platform, and the associated fault sheets, summarising the identified vulnerabilities;

e) The list of gaming software deployed on the platform, as well as the associated approval numbers provided for in Article 11.3.1 of these specifications.

12.3. Documents required only in case of modification not brought to the attention of ARJEL

The documents listed in Articles 12.3.1 to 12.3.6 shall be produced by the applicant if a modification concerning them has been made and has not been brought to the attention of ARJEL either since the license was issued or since the last certification or since the last information provided to the ARJEL services.

The absence of any modification is attested by a declaration from the operator.