AUTORITÉ NATIONALE DES JEUX

FRENCH REPUBLIC

TECHNICAL REQUIREMENTS FOR THE GAMING AND BETTING OPERATORS' INFORMATION SYSTEM AND THE OPERATOR'S LICENSING

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

Summary

In accordance with Article 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

Table of Contents

I General description

I.1 Reminder of legal and regulatory obligations

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

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

[...] Ensure integrity, reliability and transparency of gambling operations;

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. [...]”

Article 32 of Decree No 2010-518 of 19 May 2010 :

“The French Gambing Authority determines the technical requirements related to the implementation, by the operators, of the requirements set in the present chapter.“

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

I.2 Presentation of the body of documents composing the technical requirements

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 technical requirements and to divide them into five volumes in order to facilitate their appropriation by gambling operators. The present document constitutes the first of the five volumes.

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

This volume brings together the obligations that on architectural, material, organsiational , informational and procedural levels are applicable for operators with respect to the security policy of information systems.

The respect of these norms will make it possible to assess the technical and human resources used to manage the risks associated with technical and functional systems for data collection, management and storage. It must be noted that the requirements set forth in this document cover the information system as a whole, with focus points on several transverse components.

These requirements shall in particular be implemented by the operator as soon as the license is obtained for the first time or as a renewal.

Dealing comprehensively with the information system and linked to the maturity of the organisation in terms of security, this introductory and crowning volume must be read in relation the the other thematic volumes it articulates with.

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.

This volume is available under the following link :
https://ressources.anj.fr/regulation/homologation_logiciel/et2.pdf

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 defines the rules that ensure 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) (in French SMA).

It defines the information that operators must provide at all times through the physical storage medium PSM (in French SMA) 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).

This volume is available under the following link :
https://ressources.anj.fr/regulation/det/det.pdf?_=2021-002

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 is available under the following link : https://anj.fr/sites/default/files/2023-04/D%C3%A9cision%20059_FichierDesInterdits.pdf

5. Volume 5: technical requirements for certification

This section includes all the technical requirements relating to the architecture and security measures that the certifying bodies must check the actual implementation for 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.

This volume is available under the following link : https://ressources.anj.fr/regulation/certification/et5.pdf

I.3 Presentation and objectives of the 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 and betting sector, the ANJ establishes the technical characteristics of platforms and software for online gambling and betting of operators.

To this end, this document sets out the practicalities for the implementation of articles 11 and 12 of 27 March 2015 through technical requirements imposed on the operator applying for a licence or its renewal. These requirements must be understood as technical, security and organisational requirements which must necessarily complied with along the whole duration of the license. It must be noted that the requirements set forth in this document cover the information system as a whole, with focus points on several transverse components. The detailled description relates to the perimeter of the information system that provides services in relation to gambling and betting games. Other sectors of the information system such as human ressources or finances or gambling offer outside French territory are not meant to be analysed so long as they are technically decoupleand without influence on the security of the perimeter of the information system that provides services in relation to gambling and betting games.

The operators holding exclusive rights follow the requirements setdown in section IV.3 from the present document related to the ISSP (Information System Security Policy). Regarding this document, operators are remenbered that its contents and applications are analysed by the certifying body and included in the yearly certification file handed to the Authority. Besides, components of the information system common to the gaming and gambling offer under exclusive rights and the offer under licensing shall be described in the file for licensing renewal. For these components, the requirements set forth in the present document shall apply fully.

The technical IS component of licensing procedure for operators must enable the Authority to ensure:

- compliance with PSM requirements. In the case of a new operator for which the PSM would not yet be in place, the key point is to ensure that its implementation strategy incorporates the PSM requirements;

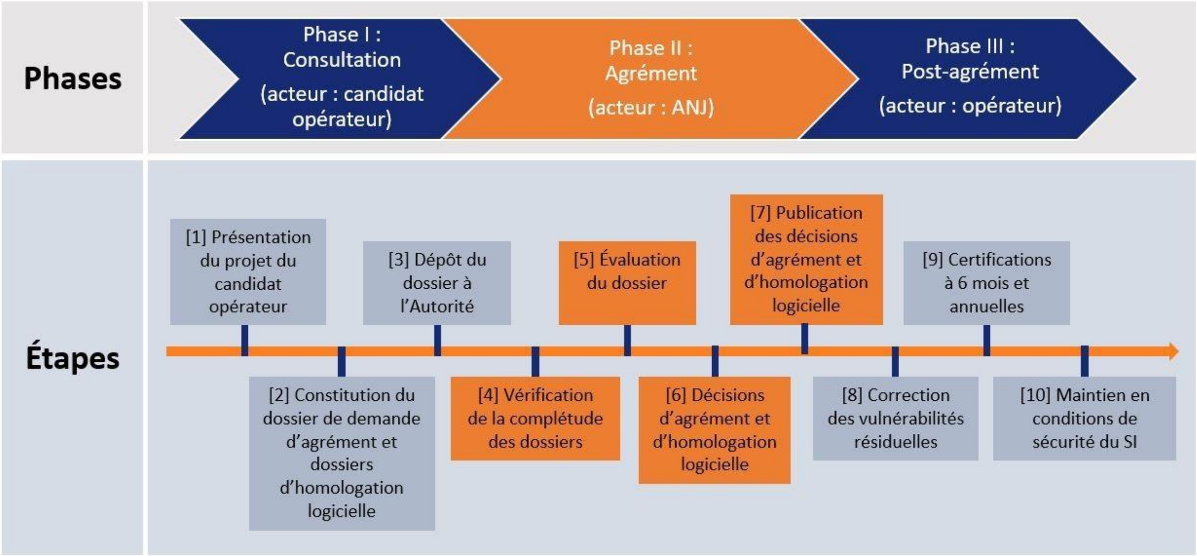
- the long-term security and robustness of the information system, both in its technical and organisational components, on which the games and related services (player account services, payments, gambling operations, etc.) are implemented by the operator.

According to the first subparagraph of Article 21(III) of the amended Law of 12 May 2010, 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 (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 Glossary

A glossary has been established, which can be found annexed to the present document, to fix a definition of terms used in one or more of the five volumes of the technical requirements, to avoid divergence of interpretations and facilitate the reading.

I.5 Identification of requirements and recommendations in the 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 Reminder of the scope of application of the license

[E_AGR_CHA1] In accordance with law No 2010-476 of 12 May 2010 on the opening-up to competition and regulation of the online gambling sector, an operator must have been delivered a license by the French Gambing Authority (ANJ) to deliver a online sport, horse-race or poker gambling and betting service in France. When instructing the file, the Authority ensures that the operator has the technical capacity to comply with legal and reglementary obligations, in particular with respect to the integrity of gaming and gambling operations and the security of information systems relied on.

[E_AGR_CHA2] An operator with a license must renew it at its expiry date. Licenses are in principle valid for 5 years. Regarding the IS component of the licensing, the renewal procedure is strictly identical to the initial licensing procedure. The file submitted to the authority shall specify what elements have changed or remained identical as compared to the previous licensing (for example, by tagging with the terms « modified »/ «unaltered » the title of a chapter or procedure that has undergone change/not undergone any change since the previous licensing.

[E_AGR_CHA3] Besides, any gaming software required for the operation of the gambling and betting offered under the license shall be approved by the Authority before the commissioning thereof.

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 they haved been 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 Expected documents and common provisions

[E_AGR_DOS1] 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 view of the architecture. This document shall be accompanied by the following annexes:
    a. an annex document presenting the PSM (sensor and vault);
    b. an annex document presenting the player account management component and player access channels;
    c. an annex document presenting IS platforms and supplier tools;
    d. an annex document setting out the processes and level of service (SLA);

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

[E_AGR_DOS2] For a new operator who has not yet finished implementing its infrastructure and processes, where some sections of the documents would either only present a forecast or be missing, the operator shall :

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

The Autority reserves the right to assess if the lacking elements do not constitute an incompleteness that would hinder the examination of the file.

[E_AGR_DOS3] Except for the case of an new operator that would not have fully implemented its infrastructure and processus yet, the différents documents must reflect the current situation at the time of filing, in particular the ISSP and master plan must correspond to the current version in force.

IV.2 Provisions for the information system master plan

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

1. Corporate strategy at 3-5 years in force;
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 deems it necessary. In the event that existing documents correspond to the content of the above-mentioned chapters, the operator provides the existing document(s) with a correspondence matrix between the above-described plan and the specific sections and pagination of the existing document(s).

[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.

This chapter must be synthetic, its goal being to give sense and context for the IT strategy.

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

1. the 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 Provisions for the document describing the information system security plan

[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 deems it necessary. In the event that existing documents correspond to the content of the above-mentioned chapters, the operator provides the existing document(s) with a correspondence matrix between the above-described plan and the specific sections and pagination of the existing document(s).

[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:

1. The start date of application of the information systems security policy;
2. The periodicity of updating the information systems security policy;
3. The strategic orientations and the level of implementation of the resulting actions;
4. The scope of application of the information systems security policy;
5. The legal and regulatory aspects related to the scope of application of the security policy;
6. The scale of requirements, which shall include a weighting and reference values in accordance with the security criteria, availability, integrity, confidentiality, tracability, along with a list of impacts backed up by examples;
7. 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;
8. Analysis of the threats selected and not selected for the scope of the study, with justifications;
9. 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 requested information shall be indicated.

   a. Information system security officer: precise definition of responsibilities, degree of formalisation, number of assistants and reporting line;
   b. 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;
   c. Internal ISS auditors: number and reporting line;
   d. ISS internal control function: number and reporting line;
   e. ISS support function: number and reporting line;
   f. ISS operational function: number and reporting line);
   g. ISS design function: number and reporting line;

   The answer may refer to the spectrum of ISS-related positions established by the French National SSI Agency (ANSSI): https://www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/

10. ISS dashboard models.

[E_AGR_SSI4] The "Human Resources" chapter describes :

1. the sensibilisation and training program for operator staff to ISS, within ISS teams and command chains and among la SSI,;
2. the advancement rate of the program ;
3. whether there exists a management and monitoring of everyone's skills ;
4. procedures to security-vet candidates applying for a sensivite position ;
5. procedures to handle conflicts of interest ;
6. procedures to guaranty information security when employees quit the company

[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:

1. Personal data of its customers;
2. Data and statistics relating to the game or certain players, knowledge of which could give a player an advantage;
3. “Secret" game data (for example other players' cards or cards that have not been turned over in a poker game) ;
4. 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:

1. 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;
2. 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;
3. 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.) ;
4. Risk studies carried out and the methodology on which these studies were based ;
5. 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:

1. Security measures for its staff;
2. The means used to protect technical premises;
3. Fire protection measures implemented;
4. The power supply redundancy policy;
5. The H24 monitoring policy of its operating sites;
6. 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. They may cover one or more functions among the following ones :
    a. Hosting centres: the type of hosting shall be precised;
    b. Interconnection centres (network nodes) : the types of interconnections used shall be precised;
    c. Operational centres (their nature shall be precised : operation team, support centre,…);
2. For gaming platforms, the sensor, and all related information systems, the license applicant shall specify:
    a. The function(s) performed;
    b. The type of data processed;
    c. The company or authority responsible for its operation;
    d. The access provider;

    e. The hosting service provider.

3. The network partitioning applied ;
4. The network filtering policy and the use of white lists ;
5. The types of network partitioning used (IP filtering, application filtering, VLAN, 802. 1X, NAP/NAC, etc.) ;
6. The security mechanisms implemented to defend against conventional IP attacks and associated protocols, in particular in relation to network denial-of-service attacks;
7. 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 sensor: The operator describes in particular the technical processes implemented (load balancing, DNS TTL adjustment, dynamic IP re-addressing of platforms, and sensor) 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 sensor : in particular the respective flows for players, gaming, technical, IT administration (both internal and external) shall be described.

[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 integrity of the following communications:

    a. Communications between the operator and the ANJ, the SMA vault in particular;
    b. Network communications between players and the operator;
    c. Network communications between modules within the physical storage medium (PSM (in French SMA)) ;

4. A description of all mechanisms and measures implemented to ensure the confidentiality and integrity of flows within its gaming platforms and physical storage medium (PSM (in French SMA)) : 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 sensor, 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. 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 communicates the contracts concluded with its service providers for the implementation of a secure development framework for the outsourced projects.

[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 security 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 vault of the physical storage medium (PSM) (in French coffre du SMA)). 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 physical storage medium (PSM (in French SMA)) context.

[E_AGR_SSI15] The "Compliance, audit, control" chapter describes the nature, periodicity, actors and methodology of ISS audits carried out on information systems and applications partaking directly or indirectly to the gaming offer. 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 Provisions for the framework document describing a comprehensive and detailed view of the architecture

[E_AGR_ARC1] the document describing the overall and detailed architecture of the IS shall 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. the list of the main software applications implemented in the scope implemented for 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 annex document presenting the PSM (see chapter below);
4. The provisions relating to the annex document presenting the player account management tool and player access channels (see chapter below);
5. The provisions relating to the annex document presenting IS platforms and supplier tools (see chapter below).
6. The provisions relating to the annex document presenting processus and service level agreements (SLA).

The document may contain additional sections if the operator deems it necessary. In the event that existing documents correspond to the content of the above-mentioned chapters, the operator provides the existing document(s) with a correspondence matrix between the above-described plan and the specific sections and pagination of the existing document(s).

IV.5 Provisions for the annex document presenting the physical storage medium (PSM) (in French 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. When implementing, it shall be taken care to respect the entire set of technical requirements defined in the volume 3 of technical requirements related to the PSM, in particular to the format applicable to data transfered into the PSM.

[E_AGR_SMA2] To do this, the company provides a document describing the PSM. This document will follow the plan detailed below:

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. Technical annexes.

The document may contain additional sections if the operator deems it necessary. In the event that existing documents correspond to the content of the above-mentioned chapters, the operator provides the existing document(s) with a correspondence matrix between the above-described plan and the specific sections and pagination of the existing document(s).

[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 for the generation of traces" 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 for the secured storage of traces” 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:

i. The submission or injection of unauthorised records;
ii. Alteration of records;
iii. Data theft;
iv. Denial of service;

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

v. Strong authentication of users and administrators;
vi. The encryption, signature and time-stamping of events;
vii. The chaining of events.

[E_AGR_SMA8] Before starting its activity, the licensed operator shall declare to the ANJ that its PSM is fully operational.

IV.6 Provisions for the annex document presenting the player account management component and player access channels

[E_AGR_GCC1] the document describes the player account management tool and access channels offered to players shall 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 deems it necessary. In the event that existing documents correspond to the content of the above-mentioned chapters, the operator provides the existing document(s) with a correspondence matrix between the above-described plan and the specific sections and pagination of the existing document(s).

[E_AGR_GCC2] The applicant company 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 company shall specify the following characteristics of his website, no matter whether it enables gaming or only acts as a portal redirecting towards a gaming service :

1. Site map;
2. Trademarks;
3. Technical characteristics of the website, domain name. 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 redirecting to a website. The applicant company shall specify whether the website offers game functions. He shall specify the planned timetable for opening these different channels.

IV.7 Provisions for the annex document presenting IS platforms and supplier tools

[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.4 Provisions for the framework document describing a comprehensive and detailed view of the architecture***, the plan detailed below :

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 deems it necessary. In the event that existing documents correspond to the content of the above-mentioned chapters, the operator provides the existing document(s) with a correspondence matrix between the above-described plan and the specific sections and pagination of the existing document(s).

[E_AGR_PLA2] the chapter « detailled architecture description » provides for each component :

1. If the component or some of its parts are subcontracted to external suppliers (this also applies if the entire platform is subcontracted);
2. The reasons for this subcontracting;
3. the contractual agreements governing these subcontracts, in particular the commitments relating to service level, responsibilities and security ;
4. controls exerted on subcontractors to ensure the IT plateforms and IS security level

[E_AGR_PLA3] Should it be a first licensing file, for each of the sections, software tools or infrastructure components 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 description of the network architecture and associated flows " chapters, written for each of the listed components, 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 shall be specified, including 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 implemented technologies 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 Provisions for the annex document setting out the processes and level of 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 deems it necessary. In the event that existing documents correspond to the content of the above-mentioned chapters, the operator provides the existing document(s) with a correspondence matrix between the above-described plan and the specific sections and pagination of the existing document(s).

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

1. the list of operating procedures used, which shall be structured by theme. The security theme will need to be clearly explicited. It shall 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;

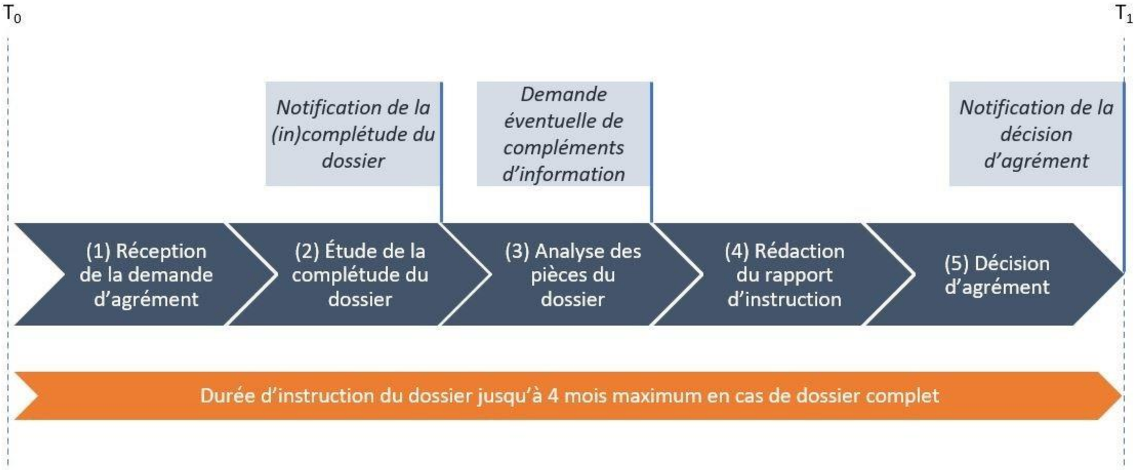
2. documentation describing the procedures listed above shall be provided. In order to facilitate the analysis, the list above shall include the precise reference (document, section, page) of each procedure in the documentation.

[E_AGR_PRO3] The “service levels (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.

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 IS component of 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 required document in a license application file must be duly justified.The file will otherwise be deeemed incomplete.

[R_AGR_PDA3] In case of doubt, it is recommended to consult the ANJ before submitting any license application in order to avoid in particular 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 the license applicant company. A preliminary exchange is required to do this where the applicant company 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 of the application

The ANJ has four months to run the instruction of the license application.app

When the application for licensing 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 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 shall 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 appropriâtes control mechanisms.

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