RÉPUBLIQUE FRANÇAISE

_____

Autorité nationale des jeux

_____

DÉCISION N° 2023-214 DU 23 NOVEMBRE 2023 PORTANT ADOPTION DES EXIGENCES TECHNIQUES RELATIVES AU SYSTEME D'INFORMATION DES OPERATEURS DE JEU ET DE L'AGREMENT

Le collège de l'Autorité nationale des jeux,

Vu la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la sécurité intérieure, notamment ses articles L. 320-3 et L. 320-4 ;

Vu la loi n° 2010-476 du 12 mai 2010 modifiée relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, notamment le VIII de son article 34 ;

Vu l'article 32 du décret 2010-518 du 19 mai 2010 modifié relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux ;

Vu l'arrêté du 27 mars 2015 portant approbation du cahier des charges applicable aux opérateurs de jeux en ligne, notamment les articles 11 et 12 de son annexe ;

Vu la notification n° 2023/0483/FR adressée à la Commission européenne le 2 août 2023 ;

Après avoir entendu le commissaire du gouvernement, en ses observations, et en avoir délibéré le 23 novembre 2023,

DÉCIDE :

Article 1er : Les exigences techniques relatives au système d'information des opérateurs de jeu et de l'agrément annexées à la présente décision sont adoptées.

Article 2 : La présente décision entre en vigueur le 1er mars 2024.

Article 3 : Le directeur général de l'Autorité nationale de jeux est chargé de l'exécution de la présente décision qui sera publiée sur le site Internet de l'Autorité.

Fait à Issy-les-Moulineaux, le 23 novembre 2023.

La Présidente de l'Autorité nationale des jeux

Isabelle FALQUE-PIERROTIN

Décision publiée sur le site de l'ANJ le 29 novembre2023

AUTORITÉ NATIONALE DES JEUX

RÉPUBLIQUE FRANÇAISE

EXIGENCES TECHNIQUES RELATIVES AU SYSTEME D'INFORMATION DES OPERATEURS DE JEU ET DE L'AGREMENT

Résumé

Conformément au VIII de l'article 34 de la loi du 12 à l'article 32 du décret n°2010-518 dans sa version applicable à compter du 1er octobre 2020, qui prévoit que le Collège de l'ANJ détermine les exigences techniques nécessaires à son application, ce document précise les exigences techniques relatives aux systèmes d'information des opérateurs de jeu.

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

Table des matières

I Présentation générale 4

I.1 Rappel des obligations légales et réglementaires 4

I.2 Présentation du corpus des exigences techniques 5

1. Volume 1 : exigences techniques relatives au système d'information et à l'agrément 5

2. Volume 2 : exigences techniques relatives à l'homologation des logiciels 5

3. Volume 3 : exigences techniques relatives à la mise à disposition des données en application des articles 31 et 38 de la loi n° 2010-476 du 12 mai 2010 5

4. Volume 4 : exigences techniques relatives à l'interrogation du ficher des Interdits de jeux ... 6

5. Volume 5 : exigences techniques relatives à la certification 6

I.3 Présentation et objectifs du document 6

I.4 Glossaire 8

I.5 Identification des exigences et recommandations dans le document 8

II Rappel du champ d'application de l'agrément 9

III Périmètre du volet SI de l'agrément 9

IV Contenu du dossier d'agrément pour le volet SI 9

IV.1 Liste des documents exigés et dispositions communes 9

IV.2 Dispositions relatives au schéma directeur du système d'information 10

IV.3 Dispositions relatives au document décrivant la politique de sécurité des systèmes d'information 11

IV.4 Dispositions relatives au document chapeau décrivant l'architecture globale et détaillée 16

IV.5 Dispositions relatives au document annexe présentant le SMA 17

IV.6 Dispositions relatives au document annexe présentant la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs 20

IV.7 Dispositions relatives au document annexe présentant les plateformes SI et briques fournisseurs 21

IV.8 Dispositions relatives au document annexe présentant les processus et niveaux de service (SLA) 24

V Procédure d'agrément d'un opérateur de jeux 25

V.1 Contenu du dossier 25

V.2 Modalités de transmission des livrables 25

V.3 Instruction de la demande 26

VI Régime de l'agrément 26

VI.1 Cycle de vie 26
VII Annexes 27
VII.1 Annexe n°1 : glossaire traverse au corpus des exigences techniques 27
VII.2 Annexe n°2 : matrices de correspondance pour les livrables du volet SI de l'agrément .. 27

I Présentation générale

I.1 Rappel des obligations légales et réglementaires

Article L. 320-3 du code de la sécurité intérieure :

« La politique de l'État en matière de jeux d'argent et de hasard a pour objectif de limiter et d'encadrer l'offre et la consommation des jeux et d'en contrôler l'exploitation afin de :

[…] 2° Assurer l'intégrité, la fiabilité et la transparence des opérations de jeu […] »

Article L. 320-4 du code de la sécurité intérieure :

« *Les opérateurs de jeux d'argent et de hasard définis à l'article L. 320-6 concourent aux objectifs mentionnés aux 1°, 2° et 3° de l'article L. 320-3. Leur offre de jeu contribue à canaliser la demande de jeux dans un circuit contrôlé par l'autorité publique et à prévenir le développement d'une offre illégale de jeux d'argent* ».

VIII de l'article 34 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne :

« L'Autorité nationale des jeux fixe les caractéristiques techniques des plates-formes et des logiciels de jeux et de paris en ligne des opérateurs soumis à un régime d'agrément et des opérateurs titulaires de droits exclusifs. Elle en évalue périodiquement le niveau de sécurité.

Elle détermine les exigences techniques en matière d'intégrité des opérations de jeux et de sécurité des systèmes d'information auxquelles doivent se conformer les opérateurs. Elle détermine les paramètres techniques des jeux en ligne pour l'application des décrets prévus aux articles 13 et 14 de la présente loi. […]

Elle évalue les contrôles internes mis en place par les opérateurs. À cette fin, elle peut procéder ou faire procéder à tout audit des systèmes d'information ou des processus. […] »

Article 32 du décret n° 2010-518 du 19 mai 2010 :

« L'Autorité nationale des jeux détermine les exigences techniques liées à la mise en œuvre, par les opérateurs, des obligations mentionnées au présent chapitre. »

Arrêté du 27 mars 2015 portant approbation du cahier des charges applicable aux opérateurs de jeu en ligne (annexe, article 11).

I.2 Présentation du corpus des exigences techniques

Afin de favoriser la lisibilité et la mise en œuvre des différentes catégories d'exigences techniques, le choix a été fait, d'une part, de les réécrire intégralement afin d'adapter le corpus des exigences techniques et de les segmenter en cinq volumes afin d'en faciliter l'appropriation par les opérateurs de jeux. Le présent document constitue le premier des 5 volumes.

1. **Volume 1 : exigences techniques relatives au système d'information et à l'agrément**

Ce volume regroupe les obligations qui, aux plans architectural, matériel, organisationnel, informationnel et procédural s'appliquent aux opérateurs en matière de politique de sécurité des systèmes d'information.

Le respect de ces normes doit permettre d'évaluer les moyens techniques et humains mis en œuvre pour gérer les risques liés aux systèmes techniques et fonctionnels de collecte, gestion et conservation des données. Il convient de noter que les exigences ici formulées portent sur l'intégralité du système d'information avec un point d'attention sur certains de ses composants transverses.

Ces exigences sont notamment mises en œuvre par l'opérateur pour l'obtention de l'agrément initial et son renouvellement.

Abordant de façon globale le système d'information et lié à la maturité de l'organisation en matière de sécurité, ce volume faîtier doit être lu en considération des autres volumes thématiques avec lesquels il s'articule.

2. **Volume 2 : exigences techniques relatives à l'homologation des logiciels**

Ce document fixe le cadre d'homologation des logiciels de jeux et de paris permettant de garantir l'intégrité et la sécurité des logiciels de jeux.

Il définit le champ d'application de l'homologation, son périmètre technique et précise le détail de la procédure, formalisant et structurant les pièces et informations attendues de la part des opérateurs.

Ce volume est disponible sous le lien suivant :
https://ressources.anj.fr/regulation/homologation_logiciel/et2.pdf.

3. **Volume 3 : exigences techniques relatives à la mise à disposition des données en application des articles 31 et 38 de la loi n° 2010-476 du 12 mai 2010**

Ce volume définit les règles garantissant l'intégrité et la cohérence de l'enregistrement des données de jeux, les modalités de mise à disposition ainsi que le formalisme des enregistrements effectués via le support matériel d'archivage (SMA).

Il définit les informations que les opérateurs doivent fournir en permanence par le biais du système matériel d'archivage (SMA) afin de permettre à l'Autorité d'exercer sa mission de contrôle permanent de l'activité des opérateurs de jeux (articles 31 et 38 de la loi n° 2010-476 du 12 mai 2010).

Ce volume est disponible sous le lien suivant :
https://ressources.anj.fr/regulation/det/det.pdf?_=2021-002

4. **Volume 4 : exigences techniques relatives à l'interrogation du ficher des Interdits de jeux**

Ce volume définit les procédures techniques (formation des clés d'interrogation, canaux et mécanismes de consultation des services DNS) à mettre en œuvre par les opérateurs afin de procéder à l'interrogation du fichier des Interdits de jeux conformément aux dispositions de l'article 22 du décret n° 2010-518 du 19 mai 2010 modifié.

Ce volume est disponible sous le lien suivant : https://anj.fr/sites/default/files/2023-04/D%C3%A9cision%20059_FichierDesInterdits.pdf

5. **Volume 5 : exigences techniques relatives à la certification**

Ce volet regroupe l'ensemble des exigences techniques relatives à l'architecture et aux mesures de sécurité dont les organismes certificateurs doivent vérifier le respect à l'occasion de la certification du SMA six mois après le lancement de l'activité et de la certification annuelle prévues par les dispositions de l'article 23 de la loi n° 2010-476 du 12 mai 2010 modifiée afin de s'assurer du maintien d'un niveau adéquat de sécurité du système.

Les volumes 1 à 5 s'appliquent tout au long de l'activité d'un opérateur.

Ce volume est disponible sous le lien suivant :
https://ressources.anj.fr/regulation/certification/et5.pdf.

I.3 Présentation et objectifs du document

Conformément aux dispositions du VIII de l'Article 34 de la loi n° 2010-476 du 12 mai 2010 modifiée relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, l'ANJ fixe les caractéristiques techniques des plates-formes et des logiciels de jeux et de paris des opérateurs.

À cette fin, le présent document définit les modalités de mise en œuvre des articles 11 et 12 de l'arrêté du 27 mars 2015 par les exigences techniques relatives pesant sur l'opérateur demandant un agrément ou son renouvellement. Les exigences posées ne s'appliquent pas exclusivement au seul moment du dépôt du dossier d'agrément mais s'entendent comme des exigences techniques, de sécurité et organisationnelles qui doivent être respectées durant l'exploitation de l'agrément. Il convient également de noter que les exigences ici formulées portent sur l'intégralité du système d'information avec un point d'attention sur certains de ses composants transverses. La description détaillée s'attache au périmètre du système d'information soutenant les jeux. D'autres pans du système d'information, ressources humaines et finances par exemple ou encore l'offre à l'international n'ont pas vocation à être analysés, dès lors que ces pans du système d'information sont techniquement découplés et sans influence sur la sécurité du périmètre du système d'information soutenant les jeux.

Les opérateurs titulaires de droits exclusifs respectent les dispositions énoncées à la Section IV.3 des présentes exigences techniques relatives à la politique de sécurité du système d'information. A cet

égard, il est rappelé qu'elle est analysée par le certificateur et remise dans le cadre du dossier de certification annuelle. Par ailleurs, tous les éléments du système d'information communs à l'offre de jeu relevant des droits exclusifs et à celle relevant d'un agrément doivent être décrits lors des renouvellements d'agrément, les exigences du présent document s'y appliquant alors pleinement.

Le volet technique de la procédure d'agrément des opérateurs doit permettre à l'Autorité de s'assurer de :

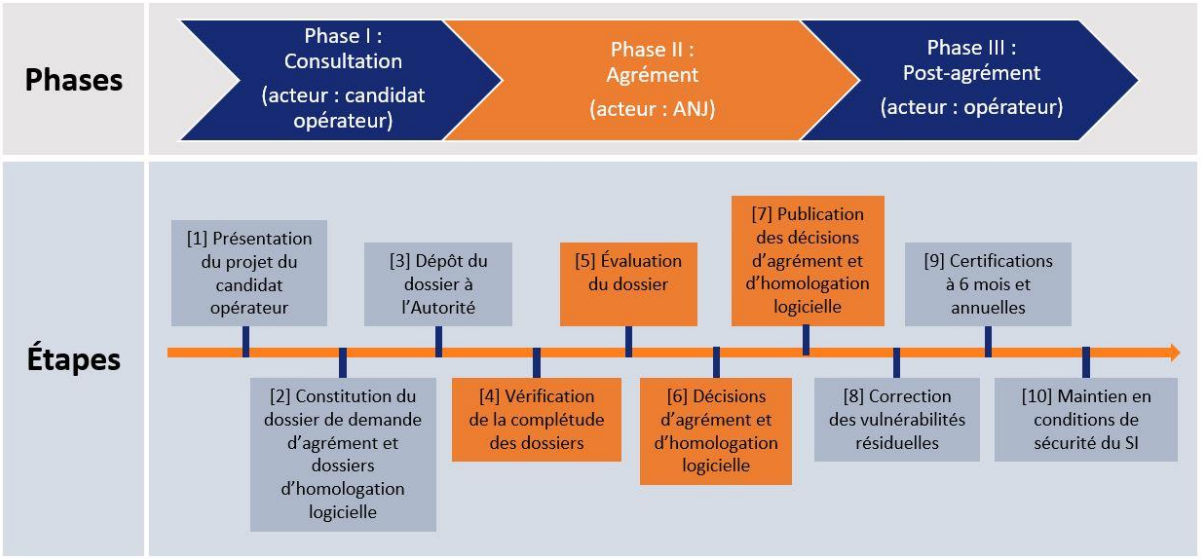
- la conformité aux exigences relatives au SMA. Dans le cas d'un nouvel opérateur pour lequel le SMA n'est pas encore en place, l'enjeu est de s'assurer que la stratégie de mise en œuvre de celui-ci intègre bien les exigences relatives au SMA ;
- la sécurité et de la robustesse du système d'information, tant dans sa composante technique qu'organisationnelle, inscrites dans la durée, sur lequel les jeux et services connexes (services de comptes joueurs, paiements, opérations de jeu, etc.) sont mis en œuvre par l'opérateur.

Il est rappelé que le premier alinéa du III de l'article 21 de la loi du 12 mai 2010 modifiée que l'Autorité peut refuser la délivrance ou le renouvellement d'un agrément « *pour un motif tiré de l'incapacité technique (…) du demandeur de faire face durablement aux obligations attachées à son activité ou de la sauvegarde de l'ordre public, de la lutte contre le blanchiment des capitaux et le financement du terrorisme, des nécessités de la sécurité publique et de la lutte contre le jeu excessif ou pathologique* ».

Le document expose :

- le champ d'application de la procédure d'agrément, c'est-à-dire dans quels cas l'opérateur doit faire une demande d'agrément (section II) ;
- le périmètre de l'agrément sur le volet SI (section III) ;
- le contenu du dossier d'agrément pour le volet SI, c'est-à-dire les documents qui le composent et les exigences relatives à chacun de ces documents en termes de contenu et d'organisation de l'information demandée (section IV)
- la procédure d'agrément (section V) ;
- les suites de l'agrément (section VI).

Les différentes phases de la procédure d'agrément sont présentées dans la figure ci-dessous :



I.4 Glossaire

Un glossaire a été établi, qui figure en annexe des présentes exigences, pour fixer la définition des termes employés dans les cinq volumes des exigences techniques, ceci afin d'éviter les divergences d'interprétation et faciliter la lecture.

I.5 Identification des exigences et recommandations dans le document

Le présent document comporte deux niveaux de préconisations :

- Les mesures précédées de **[E_numero]** sont des exigences qui revêtent un caractère **obligatoire**, sous réserve des exceptions mentionnées au sein des présentes exigences techniques ;
- Les mesures précédées de **[R_numero]** sont des recommandations, que les opérateurs peuvent décider de ne pas suivre sous réserve d'en justifier auprès de l'Autorité et d'indiquer à cette dernière les mesures alternatives qu'ils entendent mettre en place.

II Rappel du champ d'application de l'agrément

[E_AGR_CHA1] Conformément à la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, un opérateur doit disposer d'un agrément délivré par l'Autorité nationale des jeux pour proposer en France un service de jeu de cercle ou de pari sportif ou hippique en ligne. A l'occasion de l'examen de sa demande, l'ANJ s'assure notamment que l'opérateur dispose de la capacité technique à se conformer à ses obligations légales et réglementaires, notamment en ce qui concerne l'intégrité des opérations de jeu et de sécurité des systèmes d'information.

[E_AGR_CHA2] Un opérateur bénéficiant d'un agrément doit le renouveler à son échéance, la durée de l'agrément étant en principe de cinq ans. Sur le volet SI de l'agrément, la procédure de renouvellement est strictement identique à la procédure initiale de délivrance. Le dossier remis à l'autorité précise quels éléments ont évolué ou sont restés identiques par rapport au précédent agrément (par exemple en apposant entre parenthèses les termes « modifié » / « non modifié » au titre d'un chapitre ou d'une procédure qui l'a été / ne l'a pas été depuis l'agrément précédent).

[E_AGR_CHA3] Par ailleurs, tout logiciel de jeu nécessaire au fonctionnement d'une offre de jeu proposée dans le cadre de l'agrément doit avoir été homologué par l'Autorité préalablement à sa mise en service.

III Périmètre du volet SI de l'agrément

[E_AGR_PER1] Le périmètre du volet SI de l'agrément couvre l'ensemble des aspects organisationnels et techniques du SI de l'opérateur tels que qu'ils ont été mis en place (cas d'un renouvellement d'agrément) ou seront mis en place (cas d'un agrément nouveau), avec un accent particulier porté sur les composants spécifiques liés au jeu (compte joueur, SMA, …) et la sécurité du SI dans sa globalité.

IV Contenu du dossier d'agrément pour le volet SI

IV.1 Liste des documents exigés et dispositions communes

[E_AGR_DOS1] Le dossier de demande d'agrément d'un opérateur de jeu déposé auprès de l'ANJ, dans un format dématérialisé, comprend les pièces suivantes :

1. le schéma directeur du système d'information ;
2. la politique de sécurité des systèmes d'information ;
3. un document chapeau décrivant l'architecture globale et détaillée. Ledit document est accompagné des documents annexes suivants :
    a. un document annexe présentant le SMA (capteur et coffre-fort) ;
    b. un document annexe présentant la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs ;
    c. un document annexe présentant les plateformes SI et briques fournisseurs ;
    d. un document annexe présentant les processus et niveau de service (SLA).

Les dispositions relatives à chacun des documents listés ci-dessus sont détaillés dans les sections qui suivent.

[E_AGR_DOS2] Pour un nouvel opérateur n'ayant pas encore finalisé la mise en place de son infrastructure et processus et où certaines sections des documents ne présenteraient donc que le prévisionnel ou manqueraient, il doit :

1. remettre dans le dossier de demande d'agrément le calendrier de finalisation de ceux-ci ;
2. communiquer à l'Autorité les éléments complémentaires conformément au calendrier communiqué ;
3. et soumettre ces éléments à l'analyse du certificateur à la certification suivante.

Il reviendra à l'Autorité d'apprécier si les absences en question constituent une incomplétude de dossier obérant son instruction.

[E_AGR_DOS3] En dehors du cas d'un nouvel opérateur qui n'aurait pas encore intégralement mis en place l'infrastructure technique et les processus, les différents documents doivent refléter la situation technique de l'opérateur au moment du dépôt, en particulier la PSSI et le schéma directeur fournis dans le dossier doivent être les versions applicables.

L'attention de l'opérateur est appelée sur le fait que le non-respect de cette obligation **[E_AGR_DOS3]** peut conduire à rejet de la demande d'agrément.

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

[E_AGR_DIR1] Le schéma directeur du système d'information suit le plan détaillé ci-après :

1. stratégie d'entreprise à 3-5 ans en vigueur ;
2. stratégie du système d'information ;
3. organisation de la fonction système d'information ;
4. ressources humaines de la fonction système d'information ;
5. ressources budgétaires ;
6. gouvernance SI.

Le document peut contenir des sections supplémentaires si l'opérateur le juge nécessaire. Dans le cas où des documents déjà existants correspondent au contenu des chapitres demandés ci-dessus, le candidat à l'agrément fournit lesdits documents avec une matrice de correspondance entre le plan décrit ci-dessus et les sections précises paginées desdits documents.

[E_AGR_DIR2] Le chapitre « stratégie d'entreprise » décrit les éléments suivants :

1. la date d'établissement du schéma directeur, la période couverte et les dates de mises à jour prévisionnelles sont précisées.
2. la stratégie de l'entreprise sur un horizon temporel de 3 à 5 ans en présentant contexte, ambition et positionnement ;
3. les enjeux métiers déclinant cette cible.

Ce chapitre a vocation à être très synthétique, il a essentiellement pour fonction de donner sens et contexte à la stratégie du système d'information.

[E_AGR_DIR3] Le chapitre « stratégie du système d'information » décrit les éléments suivants :

1. les principes directeurs IT couvrant tout le périmètre porté par le SI ;
2. les projets SI structurants répondant aux enjeux métiers, leur objectif détaillé, phasage éventuel et leur calendrier. La composante SSI dans chaque projet doit être explicitée.
3. pour les projets lancés, une synthèse de l'avancement à date est jointe.

[E_AGR_DIR4] Le chapitre « organisation de la fonction système d'information » contient au moins les éléments suivants :

1. les différentes structures qui la composent, avec leurs missions précises ;
2. les éventuelles entités qui lui sont rattachées, avec leurs fonctions respectives et leurs implantations géographiques.

[E_AGR_DIR5] Le chapitre « ressources humaines de la fonction système d'information » contient au moins les éléments suivants :

1. les effectifs internes et équivalent temps plein (ETP) correspondants par structures et missions de la fonction système d'information sont précisés, en distinguant *a minima* les fonctions exploitation, sécurité du système d'information, projets infrastructure, projets applicatifs & MCO, pilotage & stratégie ;
2. le cas échéant, les évolutions des effectifs prévues sur l'horizon temporel du schéma directeur ;
3. la politique d'externalisation applicable à la fonction système d'information ;
4. elle précise les métiers ou fonctions faisant appel à la sous-traitance ou à l'externalisation (notamment hébergement web, infogérance, sécurité, …) et les volumes (ETP) correspondants.

[E_AGR_DIR6] Le chapitre « Ressources budgétaires » contient au moins les éléments suivants :

1. le budget global SI prévisionnel annuel sur l'horizon temporel du schéma directeur ;
2. sa répartition prévisionnelle par grands domaines (fonction exploitation, sécurité du système d'information, projets infrastructure, projets applicatifs & MCO), par année sur la période couverte par le schéma directeur ;
3. sa répartition prévisionnelle annuelle sur l'horizon temporel du schéma directeur par projets SI structurants déclinant la stratégie SI.

[E_AGR_DIR7] Le chapitre « gouvernance SI » décrit les éléments suivants :

1. les acteurs de la gouvernance SI, leurs rôles et responsabilités respectives ;
2. la comitologie mise en place pour le pilotage du portefeuille des projets SI, incluant en particulier les projets structurants mentionnés au chapitre « stratégie du système d'information ».

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

[E_AGR_SSI1] La politique de sécurité des systèmes d'information (PSSI) suit le plan détaillé ci-après :

1. politique, organisation, gouvernance ;
2. ressources humaines ;
3. gestion des biens ;

4. intégration de la sécurité des systèmes d'information dans le cycle de vie des projets ;
5. sécurité physique ;
6. sécurité des réseaux ;
7. architecture des systèmes d'information ;
8. exploitation des systèmes d'information ;
9. sécurité du poste de travail ;
10. sécurité du développement des systèmes ;
11. traitements des incidents ;
12. continuité d'activité ;
13. conformité, audit, contrôle.

Le document peut contenir des sections supplémentaires si l'opérateur le juge nécessaire. Dans le cas où des documents déjà existants correspondent au contenu des chapitres demandés ci-dessus, le candidat à l'agrément fournit lesdits documents avec une matrice de correspondance entre le plan décrit ci-dessus et les sections précises paginées desdits documents.

[E_AGR_SSI2] Les documents d'application ou procédures techniques détaillées déclinant les exigences posées par la politique de sécurité sont fournies, en précisant les moyens organisationnels et techniques correspondants mis en œuvre et leur suivi dans le temps.

[E_AGR_SSI3] Le chapitre « Politique, organisation, gouvernance » décrit :

1. la date de début d'application de la politique de sécurité des systèmes d'information ;
2. la périodicité de mise à jour de la politique de sécurité des systèmes d'information ;
3. les orientations stratégiques ainsi que le niveau de réalisation des actions en découlant ;
4. le périmètre d'application de la politique de sécurité des systèmes d'information ;
5. les aspects légaux et réglementaires liés au périmètre d'application de la politique de sécurité ;
6. l'échelle de besoins, qui comporte une pondération et des valeurs de référence selon les critères de sécurité disponibilité intégrité confidentialité traçabilité (DICT), ainsi qu'une liste d'impacts enrichis d'exemples ;
7. la description des besoins de sécurité des domaines d'activité de l'opérateur, selon l'échelle de besoins présentée dans la partie précédente ;
8. l'analyse des menaces retenues et non retenues pour le périmètre de l'étude, avec des justifications ;
9. une description de l'organisation mise en place pour assurer la sécurité des systèmes d'information, ainsi que la sécurité physique des locaux. L'existence des fonctions suivantes est indiquée ainsi que les informations demandées :
    a. responsable sécurité du système d'information : définition précise des responsabilités, degré de formalisation, nombre d'adjoints et rattachement hiérarchique ;
    b. autorité d'exploitation du système d'information (SI) (ou fonction équivalente) : définition précise des responsabilités, degré de formalisation et, le cas échéant, nature des responsabilités en matière de sécurité des systèmes d'information (SSI) ;
    c. auditeurs internes en SSI : nombre et rattachement hiérarchique ;
    d. fonction de contrôle interne en SSI : nombre et rattachement hiérarchique ;
    e. fonction support en SSI : nombre et rattachement hiérarchique ;
    f. fonction opérationnelle en SSI : nombre et rattachement hiérarchique) ;
    g. fonction de conception en SSI : nombre et rattachement hiérarchique.

La réponse pourra s'appuyer sur le panorama des métiers de la cybersécurité proposé par l'ANSSI : https://www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/

10. Les modèles de tableaux de bord SSI.

[E_AGR_SSI4] Le chapitre « Ressources Humaines » décrit :

1. le programme de sensibilisation et de formation du personnel de l'opérateur à la SSI, dans les chaînes SI, SSI et parmi les utilisateurs métier ;
2. le taux d'avancement du programme ;
3. s'il existe une gestion et un suivi régulier de la compétence de chacun ;
4. les procédures de vérification des candidats postulant à un poste sensible ;
5. les procédures de gestion des conflits d'intérêt ;
6. les procédures de mises en sécurité de l'information lors du départ de salariés de la société.

[E_AGR_SSI5] Le chapitre « Gestion des biens » décrit les procédures et mécanismes mis en place afin de protéger les données traitées par l'opérateur, notamment :

1. les données nominatives et personnelles de ses clients ;
2. les données et statistiques de jeu ou de certains joueurs dont la connaissance pourrait avantager un joueur ;
3. les données de jeu " secrètes " (par exemple les cartes des autres joueurs ou celles qui n'ont pas été retournées lors d'une partie de poker) ;
4. les modalités d'identification et de classification des composants sensibles (y compris les données) et la méthodologie afférente.

[E_AGR_SSI6] Le chapitre « Intégration de la SSI dans le cycle de vie des projets » décrit :

1. la gestion de la sécurité mis en œuvre par l'opérateur à chaque étape du cycle de développement des systèmes, dans les phases de définition, de développement, d'exploitation et d'utilisation, puis de maintenance et d'évolution. L'opérateur expose sa politique en cas de vulnérabilité identifiée et d'absence de correctifs ;
2. la procédure de recette SSI relative aux projets de systèmes d'information avant leur mise en service et précise la proportion des systèmes d'information ayant effectivement fait l'objet d'une telle recette ;
3. les modalités de mise en œuvre de tout examen formalisé d'impact sur la sécurité d'un SI ou sur la mise en exploitation d'un nouveau composant (modèle de serveur, système d'exploitation, application, données, etc.) ;
4. les études de risques réalisées et la méthodologie sur la base de laquelle ces études reposent ;
5. les contrôles exercés auprès des sous-traitants afin d'assurer un maintien du niveau de sécurité de ses plates-formes et systèmes d'information.

[E_AGR_SSI7] Le chapitre « Sécurité physique » décrit :

1. les mesures de sécurité concernant son personnel ;
2. les moyens mis en œuvre aux fins de protection des locaux techniques ;
3. les moyens mis en œuvre de protection incendie ;
4. la politique de redondance en alimentation électrique ;
5. la politique de surveillance H24 de ses sites en exploitation ;
6. la politique de gestion des accès physiques.

[E_AGR_SSI8] Le chapitre « Sécurité des réseaux » décrit :

1. les centres d'exploitation et de supervision informatiques et réseau : leur localisation, les applications hébergés et le personnel affecté. Ils peuvent couvrir une ou plusieurs fonctions parmi celles de :
    a. centres d'hébergement : préciser le type d'hébergement ;
    b. centres d'interconnexion (nœuds réseaux) : préciser les types d'interconnexion utilisés ;
    c. les centres opérationnels (préciser la nature : équipes d'exploitation, centre support,…) ;
2. pour les plates-formes de jeux, le capteur, et l'ensemble des systèmes d'information afférents à ceux-ci, le candidat à l'agrément précise :
    a. la ou les fonctions assurées ;
    b. le type de données traitées ;
    c. l'entreprise ou l'autorité responsable de son exploitation ;
    d. le fournisseur d'accès ;
    e. l'hébergeur ;
3. le cloisonnement du réseau appliqué ;
4. la politique de filtrage réseau et l'utilisation de listes blanches ;
5. les typologies de cloisonnement réseau employés (filtrage IP, filtrage applicatif, VLAN, 802. 1X, NAP/ NAC, etc.) ;
6. les mécanismes de sécurité mis en œuvre afin d'assurer une défense contre les attaques classiques sur IP et les protocoles associés, en particulier par rapport aux attaques en déni de service réseau ;
7. les mesures techniques et organisationnelles prises en termes de résilience réseau de ses systèmes d'information, notamment au regard de la lutte contre les attaques en déni de service (distribuées ou non, par épuisement de bande passante, ou encore de ressources système) au niveau des plates-formes de jeux et du capteur : l'opérateur décrit notamment les procédés techniques mis en œuvre (équilibrage de charge, ajustement des TTL DNS, ré-adressage IP dynamique des plates-formes, et du capteur) et les mesures organisationnelles associées (remontée d'alerte en cas d'attaque, protocole d'accord avec les FAI pour la lutte contre les DDOS, etc.).

[E_AGR_SSI9] Le chapitre « Architecture des SI » décrit l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux au sein de ses plates-formes de jeux et du capteur : il convient de couvrir les flux joueurs, les flux métiers, les flux techniques, les flux administration (internes et externes).

[E_AGR_SSI10] Le chapitre « Exploitation des SI » décrit :

1. les mécanismes d'identification et d'authentification des joueurs ;
2. les mécanismes de contrôle d'accès des joueurs : détails des éventuels profils de joueurs et mécanismes de cloisonnement des droits ;
3. les procédés cryptographiques permettant de garantir l'authentification des composants, la confidentialité et l'intégrité des communications suivantes :
    a. les communications entre l'opérateur et l'ANJ, en particulier le coffre ;
    b. les communications réseaux entre joueurs et l'opérateur ;

c. les communications réseaux entre les modules au sein du système matériel d'archivage (SMA) ;

4. la description de l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux au sein de ses plates-formes de jeux et du système matériel d'archivage (SMA) : ces flux concernent les administrateurs faisant partie du personnel de l'opérateur tels les exploitants par exemple, les administrateurs externes tels ceux qui assurent la télémaintenance des matériels, etc. ;
5. la description des mécanismes d'accès aux fonctions d'administration de la plateforme de jeu et du capteur ;
6. les mesures mises en œuvre lui permettant de garantir un haut niveau de sécurité dans la gestion des secrets d'authentification (notamment, robustesse des mots de passe, changement périodique, authentification forte) pour les personnels exploitant de l'opérateur ;
7. le processus d'application des correctifs, et notamment en cas de régression constatée ;
8. les procédures techniques permettant un retour en arrière dans le cas où un correctif provoquerait une éventuelle régression ;
9. la description de la journalisation et la durée de conservation.

[E_AGR_SSI11] Le chapitre « Sécurité du poste de travail » décrit :

1. la procédure de fourniture et la politique de gestion des postes de travail du candidat ;
2. la procédure formalisée de configuration des postes de travail ;
3. les mécanismes de protection contre le vol ;
4. la gestion des privilèges sur les postes de travail ;
5. la gestion des accès en nomadisme tel que le télétravail ;
6. la gestion des supports de stockage amovibles.

[E_AGR_SSI12] Le chapitre « Sécurité du développement des systèmes » décrit :

1. les moyens que l'opérateur met en œuvre pour protéger les données à caractère personnel et la vie privée des joueurs ;
2. les mesures de contrôle et méthodes d'évaluation de ses développements à chaque étape d'un projet de développement ;
3. le référentiel de développement sécurisé pour les projets dont l'opérateur assure le développement.

L'opérateur communique les contrats conclus avec ses prestataires relatifs à la mise en place d'un référentiel de développement sécurisé pour les projets dont il externalise la prise en charge.

[E_AGR_SSI13] Le chapitre « Traitement des incidents » décrit :

1. le mode de fonctionnement du centre opérationnel chargé de la SSI de l'opérateur. Il précise notamment le rattachement hiérarchique, le régime de veille et l'effectif de permanence. A défaut, il précise les modalités de veille et de déclenchement des alertes ;
2. les procédures mises en place en vue de traiter les cas d'incident de sécurité et de détection de fraude. Elle précise le niveau de diffusion de ces documents ainsi que les modalités d'alerte prévues.
3. l'état des incidents de SSI ou des fraudes que l'opérateur aurait pu constater. Il en précise les occurrences (notamment l'identification des sources d'entrée et du niveau) et la gestion qui en a été faite ;

4. les solutions mises en œuvre pour éviter ou détecter, le cas échéant, les attaques et intrusions sur ses systèmes d'information.

[E_AGR_SSI14] Le chapitre « Continuité d'activité » décrit :

1. le service d'archivage en vue d'assurer la conservation de l'ensemble de ses données de traitement et en particulier celles stockées dans le coffre-fort du système matériel d'archivage (SMA). L'opérateur précise le type de support et le format de la sauvegarde ;
2. les mécanismes d'archivage ainsi que les moyens sécurisés de protection des archives que l'opérateur est capable de mettre en œuvre ;
3. les modalités de son plan de sauvegarde. L'opérateur précise en particulier les modalités et les délais de restauration d'une sauvegarde à la suite d'un incident ainsi que le ou les lieux de stockage des sauvegardes et les mesures de sécurité appliquées à ce(s) lieu(x) ;
4. les plans de continuité d'activité et plans de reprise d'activité que l'opérateur a pu élaborer dans le cadre de son activité et les modalités qu'elle prévoit pour les adapter au contexte du système matériel d'archivage ;
5. les procédures de reprise et continuité d'activité (PRA et PCA) si non directement intégrées aux plans.

[E_AGR_SSI15] Le chapitre « Conformité, audit, contrôle » décrit la nature, la périodicité, les acteurs et la méthodologie des audits SSI réalisés sur les systèmes d'information et les applications impliquées directement ou indirectement dans le service de jeu offert. L'opérateur en communique les comptes rendus et les principales recommandations. Il précise les modalités de décision des mesures correctrices et celles de leur mise en œuvre et du contrôle de leur bonne exécution. Il indique la proportion des mesures réellement appliquées.

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

[E_AGR_ARC1] le document décrivant l'architecture globale et détaillée du SI suit le plan détaillé ci-après :

1. la description générale de la plateforme du système d'information :
    a. l'ensemble des composants mis en œuvre dans le SI et, pour chacun, la ou les fonctions qu'il assure ;
    b. le type d'hébergement de chaque composant ;
    c. l'ensemble des interconnexions entre composants et, pour chacune, en décrire la finalité de telle sorte que soit défini comment les composants collaborent pour assurer le fonctionnement global du système ;
    d. l'entreprise ou l'autorité responsable de l'exploitation de chaque composant.
    e. les centres d'exploitation et de supervision informatiques et réseau en précisant la ou leurs localisations, les modes de fonctionnement ainsi qu'une estimation du volume d'ETP mis en œuvre ;
    f. les centres d'hébergement (localisation, type d'hébergement) ;
    g. les centres d'interconnexion (types, fournisseurs) ;

h. les centres opérationnels (notamment centre de sécurité, centre service client, centre de service pour le développement, …) ;
i. les fournisseurs d'accès réseau pour chaque liaison sortant/entrant dans le SI ;
j. la liste des principaux logiciels mis en œuvre dans le cadre des activités liées aux agréments ou activités visées est précisée ;

2. la présentation globale de l'architecture avec schémas réseau logique et physique, schémas applicatifs, la cartographie du réseau ;
3. les dispositions relatives au document annexe présentant le SMA (voir chapitre ci-dessous) ;
4. les dispositions relatives au document annexe présentant la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs (voir chapitre ci-dessous) ;
5. les dispositions relatives au document annexe présentant les plateformes SI et briques fournisseurs (voir chapitre ci-dessous) ;
6. les dispositions relatives au document annexe présentant les processus et niveaux de service (SLA).

Le document peut contenir des sections supplémentaires si l'opérateur le juge nécessaire. Dans le cas où des documents déjà existants correspondent au contenu des chapitres demandés ci-dessus, le candidat à l'agrément fournit lesdits documents avec une matrice de correspondance entre le plan décrit ci-dessus et les sections précises paginées desdits documents.

IV.5 Dispositions relatives au document annexe présentant le SMA

[E_AGR_SMA1] Au moment du dépôt du dossier de demande d'agrément, le SMA n'est pas nécessairement en fonctionnement. L'entreprise doit néanmoins être en mesure de présenter sa stratégie détaillée de mise en œuvre prévue pour celui-ci dans le cadre de la collecte et la sauvegarde de la totalité des données qu'il sert à recueillir. Lors de l'implémentation concrète, elle veille à respecter l'ensemble des exigences opérationnelles formulées dans le volume 3 des exigences techniques relatives au SMA et en particulier aux formats applicables aux données qui y sont versées.

[E_AGR_SMA2] Pour ce faire, l'entreprise fournit un document décrivant le SMA. Ce document suit le plan détaillé ci-après:

1. description générale du SMA ;
2. description détaillée du capteur pour la génération des traces ;
3. description détaillée du coffre-fort pour le stockage sécurisé des traces ;
4. description des fonctions d'accès aux traces recueillies par le SMA ;
5. annexes techniques.

Le document peut contenir des sections supplémentaires si l'opérateur le juge nécessaire. Dans le cas où des documents déjà existants correspondent au contenu des chapitres demandés ci-dessus, le candidat à l'agrément fournit lesdits documents avec une matrice de correspondance entre le plan décrit ci-dessus et les sections précises paginées desdits documents.

[E_AGR_SMA3] Le chapitre « Description générale du SMA (coffre-fort et capteur) » contient les sections suivantes :

1. la stratégie globale employée : il s'agit de présenter le fonctionnement général mis en œuvre ou envisagé, s'agissant de la collecte et le stockage sécurisé des traces ;

2. l'architecture générale, présentant les différents composants du SMA, leur rôle, leur positionnement par rapport à la plateforme de jeu ainsi que leurs interactions avec la plateforme de jeu, les joueurs et tout autre éventuel SI.

[E_AGR_SMA4] Le chapitre « Description détaillée du capteur pour la génération des traces » contient les sections suivantes :

Cadrage global :

1. la stratégie détaillée employée pour le capteur relative à la génération des traces. Il s'agit de présenter la solution de capteur retenue et le fonctionnement associé vis-à-vis des données échangées dont les traces sont exigées (exemple : choix d'un capteur fonctionnant en coupure du flux applicatif entre le joueur et la plateforme de jeu concernant les requêtes émises par le joueur) ;
2. la stratégie employée vis-à-vis de la très haute disponibilité demandée, précisant les mesures mises en œuvre en cas d'indisponibilité ou dysfonctionnement du capteur ;
3. l'analyse de risques conduite concernant le capteur ;
4. la politique de sécurité applicable incluant une description détaillée des mesures de sécurisation du capteur ;
5. le capteur au sens logique peut être constitué de plusieurs capteurs physiques, potentiellement de types différents. La description demandée doit être déclinée pour chaque type de capteurs physiques mis en œuvre.

Réalisation :

6. l'identité et les coordonnées du (ou des) prestataire(s) réalisant le développement, la maintenance du capteur ou du fournisseur de la solution de capteur retenue ;
7. les spécifications détaillées du capteur dont :
    a. l'architecture fonctionnelle et technique (applicative et réseau) détaillée du capteur ;
    b. les spécifications des interfaces et le cas échéant des fonctions de « proxy » (du flux applicatif) implémentées par le du capteur ;
    c. la description des différents flux (i.e. type de données, protocoles) transitant par le capteur ;
    d. la description détaillée des mécanismes mis en œuvre relatifs à l'acquittement (positif ou négatif) des traces par la plateforme de jeux et par le coffre-fort ;
    e. la description détaillée des mécanismes mis en œuvre relatifs au traitement par lot des traces, s'agissant de la communication des traces au coffre-fort ;
    f. la description détaillée des mécanismes d'authentification et de confidentialité mis en place dans le cadre des échanges de données :
        - entre le joueur et le capteur ;
        - entre le capteur et la plateforme de jeu ;
8. lorsque le SMA est d'ores et déjà mis en place, la liste et les résultats des tests d'audits effectués ;

Hébergement :

9. la localisation physique du capteur ;
10. les modalités d'hébergement du capteur ;
11. l'identité et les coordonnées du prestataire réalisant l'hébergement du capteur ;
12. la production du ou des contrats d'hébergement ;

13. les documents d'administration et d'exploitation du capteur ;
14. les procédures mises en place notamment en termes de protection contre les accès non autorisés.

[E_AGR_SMA5] Le chapitre « Description détaillée du coffre-fort pour le stockage sécurisé des traces » contient les sections suivantes :

Cadrage global :

1. la stratégie détaillée employée pour le stockage sécurisé des traces. Il s'agit de présenter la solution de coffre-fort retenue et le fonctionnement associé ;
2. la stratégie employée vis-à-vis de la très haute disponibilité demandée, précisant les mesures mises en œuvre en cas d'indisponibilité du coffre-fort ;
3. l'analyse de risques conduite concernant le coffre-fort ;
4. la politique de sécurité applicable dont la description détaillée des mesures de sécurisation du coffre-fort.

Réalisation :

5. l'identité et les coordonnées du (ou des) prestataire(s) réalisant le développement, la maintenance du coffre-fort ou du fournisseur de la solution de coffre-fort retenue ;
6. les spécifications détaillées du coffre-fort dont :
    a. l'architecture fonctionnelle et technique détaillée du coffre-fort ;
    b. la description détaillée des mécanismes d'authentification et de confidentialité mis en place concernant l'échange de données :
        - entre le capteur et le coffre-fort ;
        - entre le coffre-fort et le système d'information de l'ANJ ;
    c. la description des différents algorithmes employés pour le stockage sécurisé des traces (exemple : chaînage des traces).
7. lorsque le SMA est d'ores et déjà mis en œuvre, la liste et les résultats des rapports de tests effectués.

Hébergement :

8. la localisation physique du coffre-fort (celui-ci devant être hébergé en France métropolitaine conformément à l'article 31 de la loi n°2010-476 du 12 mai 2010) ;
9. les modalités d'hébergement du coffre-fort ;
10. l'identité et les coordonnées du prestataire réalisant l'hébergement du coffre-fort ;
11. la production du ou des contrats d'hébergement ;
12. les documents d'administration et d'exploitation du coffre-fort dont en particulier :
    a. la spécification précise du déroulement de la cérémonie envisagée d'initialisation du coffre et de remise des clés nécessaire ;
    b. la spécification et rôle des bi-clés utilisées ;
    c. la description détaillée des mécanismes d'authentification des personnes physiques au coffre ;
    d. la description détaillée des fonctions d'administration et de gestion des utilisateurs du coffre-fort.
13. les procédures mises en place notamment en termes de protection contre les accès non autorisés.

[E_AGR_SMA6] Le chapitre « Description des fonctions d'accès aux traces recueillies par le SMA » contient les sections suivantes :

1. la description détaillée de l'outil de consultation et de collecte à distance des fichiers de traces, dont :
    a. les spécifications détaillées fonctionnelles et techniques ;
    b. lorsque le SMA est d'ores et déjà mis en œuvre, les rapports des tests effectués ;
2. la description détaillée de l'outil de validation et d'extraction des fichiers de traces, dont :
    a. les spécifications détaillées fonctionnelles et techniques ;
    b. lorsque le SMA est d'ores et déjà mis en œuvre, les rapports des tests effectués.

[E_AGR_SMA7] Le chapitre « Annexes techniques » contient :

1. lorsque le SMA est d'ores et déjà mis en place :
    a. le code source du capteur ;

    l'Autorité se réserve le droit de demander en outre, lors de l'instruction de l'agrément ou ultérieurement :
    b. le code source du coffre-fort ;
    c. le code source de l'outil de consultation et de collecte à distance des fichiers de traces ;
    d. le code source de l'outil de validation et d'extraction des fichiers de traces ;
2. une copie du certificat de sécurité a minima de premier niveau (CSPN) et ses éventuels rapports de maintenance du coffre-fort du SMA (ou du calendrier d'obtention accompagné d'une note du centre d'évaluation ou du centre de certification attestant que la procédure de certification a été engagée) ;
    a. la CSPN doit au minimum prendre en compte les éléments suivants, au niveau des menaces :
        i. le dépôt ou l'injection d'enregistrements non autorisés ;
        ii. l'altération d'enregistrements ;
        iii. le vol de données ;
        iv. le déni de service ;
    b. la CSPN doit à minimum prendre en compte les éléments suivants, au niveau des fonctions de sécurité :
        v. l'authentification forte des utilisateurs et administrateurs ;
        vi. le chiffrement, la signature et l'horodatage des évènements ;
        vii. le chaînage des évènements.

[E_AGR_SMA8] Avant de débuter son activité, l'opérateur agréé déclare à l'ANJ que son SMA est pleinement opérationnel.

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] le document décrit la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs suit le plan détaillé ci-après :

1. modalités techniques d'accès et d'inscription au site de tout joueur ;

2. moyens techniques permettant de s'assurer de l'identité de chaque nouveau joueur, de son âge, de son adresse et de l'identification du compte de paiement sur lequel sont reversés ses avoirs ;
3. modalités techniques d'encaissement et de paiement, à partir de son site, des mises et des gains.

Le document peut contenir des sections supplémentaires si l'opérateur le juge nécessaire. Dans le cas où des documents déjà existants correspondent au contenu des chapitres demandés ci-dessus, le candidat à l'agrément fournit lesdits documents avec une matrice de correspondance entre le plan décrit ci-dessus et les sections précises paginées desdits documents.

[E_AGR_GCC2] Le candidat justifie de l'obtention au moins d'un nom de domaine de premier niveau comportant la terminaison « .fr » par la production d'un certificat d'enregistrement. Il déclare, le cas échéant, tous les autres noms de domaine de premier niveau comportant la terminaison ". fr " qu'il entend exploiter pour l'accès à son site de jeux en ligne et fournit les pièces justifiant des enregistrements correspondants.

[E_AGR_GCC3] Le candidat précise les caractéristiques de son site suivantes, que le site permette le jeu ou ne constitue qu'un portail de redirection :

1. plan du site ;
2. marques ;
3. caractéristiques techniques du site, nom de domaine.la description détaillée du site « .fr » mis en place :
    a. hébergeur ;
    b. localisation ;
    c. code source ;
    d. politique de sécurité ;
    e. analyse de risques ;
    f. procédures d'administration, d'exploitation et de sécurisation mises en place ;
4. la description détaillée des fonctions de redirection des connexions de joueurs.

[E_AGR_GCC4] Le candidat précise les canaux de jeux prévus, qui permettront aux clients de jouer : clients lourds, applications natives sur smartphone complètes ou redirigeant vers un site web. Le candidat précise si le site web offre des fonctionnalités de jeu. Il précise le calendrier prévisionnel d'ouverture de ces différents canaux.

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

[E_AGR_PLA1] le document annexe décrivant la plateforme SI de l'Entreprise suivra, pour chacun des composants identifiés dans le cadre de l'exigence **[E_AGR_ARC1]** décrite au paragraphe IV.4 ***Dispositions relatives au document chapeau décrivant l'architecture globale et détaillée***, le plan détaillé ci-après :

1. un descriptif d'architecture détaillé de chacun des composants du SI listés dans le document chapeau conformément à l'exigence **[E_AGR_ARC1]** ;

2. un descriptif détaillé de l'architecture réseau et des flux associés.

Le document peut contenir des sections supplémentaires si l'opérateur le juge nécessaire. Dans le cas où des documents déjà existants correspondent au contenu des chapitres demandés ci-dessus, le candidat à l'agrément fournit lesdits documents avec une matrice de correspondance entre le plan décrit ci-dessus et les sections précises paginées desdits documents.

[E_AGR_PLA2] Le chapitre « descriptif d'architecture détaillé » de chaque composant précise »:

1. si le composant ou certaines de ses parties sont sous-traités à des fournisseurs externes (ceci vaut également dans le cas où l'ensemble de la plateforme est sous-traitée) ;
2. les motifs ayant conduit à la sous-traitance ;
3. les accords contractuels encadrant ces sous-traitances et en particulier les engagements en matière de niveau de service, de responsabilités et de sécurité ;
4. les contrôles exercés auprès des sous-traitants afin d'assurer un maintien du niveau de sécurité de ses plates-formes et systèmes d'information.

[E_AGR_PLA3] Dans le cas d'un premier agrément, pour chacune des sections, sont prises en compte au même titre que les composants déjà en production, les briques logicielles ou éléments d'infrastructure qui seraient en chantier ou non encore opérationnels, comme s'ils étaient déjà en production pour le périmètre mis en œuvre concernant les agréments ou les activités visées.

[E_AGR_PLA4] Les chapitres « descriptif détaillé de l'architecture réseau et des flux associés», rédigés pour chacun des composants listés comprennent :

1. la description détaillée du composant, mettant en évidence chacune de ses constituantes physique et logique avec pour chaque :
    a. la ou les fonctions assurées ;
    b. le type de données traitées ;
    c. l'entreprise ou l'autorité d'exploitation désignée ;
    d. le cas échéant, les moyens de chiffrement mis en œuvre ;
    e. l'importance de sa fonction (de " outil facilitant le travail " à " outil indispensable ") ;
    f. l'importance de sa disponibilité (de " aucun effet " à " effet bloquant " en cas d'arrêt total ou partiel du système) ;
    g. l'importance de l'intégrité des données (de " aucun effet " à " effet bloquant " en cas de modification de données) ;
    h. l'importance de la confidentialité des données (de " aucun effet " à " effet bloquant " en cas de divulgation de données) ;
    i. la durée de vie prévue.
2. une description technique détaillée du réseaux, dans la description duquel sont précisés les éléments relatifs à la segmentation et aux filtrages. Figurent les descriptions des réseaux opérationnels, mais également celles des réseaux supportant l'administration et la supervision :
    a. un schéma technique du réseau ;
    b. la liste des différents flux associés ;
    c. la liste des zones de sensibilités différentes :
        i. typologie (Internet ou réseau dédié…) ;
        ii. sensibilité ;
    d. la liste descriptive des interconnexions de ces zones (rôle et finalité) ;

e. l’ensemble des technologies mises en œuvre est listé ;
f. la liste des liens vers l'extérieur (lignes dédiées, interconnexions de réseaux …) et les accès distants possibles depuis l'extérieur avec pour chacun un descriptif précis des technologies protocoles et mesures de sécurité mis en œuvre.

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

[E_AGR_PRO1] Le document annexe présentant les processus et niveaux de service suit le plan en deux chapitres ci-après :

1. procédures d'administration et d'exploitation ;
2. niveaux de service (SLA).

Le document peut contenir des sections supplémentaires si l'opérateur le juge nécessaire. Dans le cas où des documents déjà existants correspondent au contenu des chapitres demandés ci-dessus, le candidat à l'agrément fournit lesdits documents avec une matrice de correspondance entre le plan décrit ci-dessus et les sections précises paginées desdits documents.

[E_AGR_PRO2] Le chapitre « procédures d'administration et d'exploitation » décrit les éléments suivants :

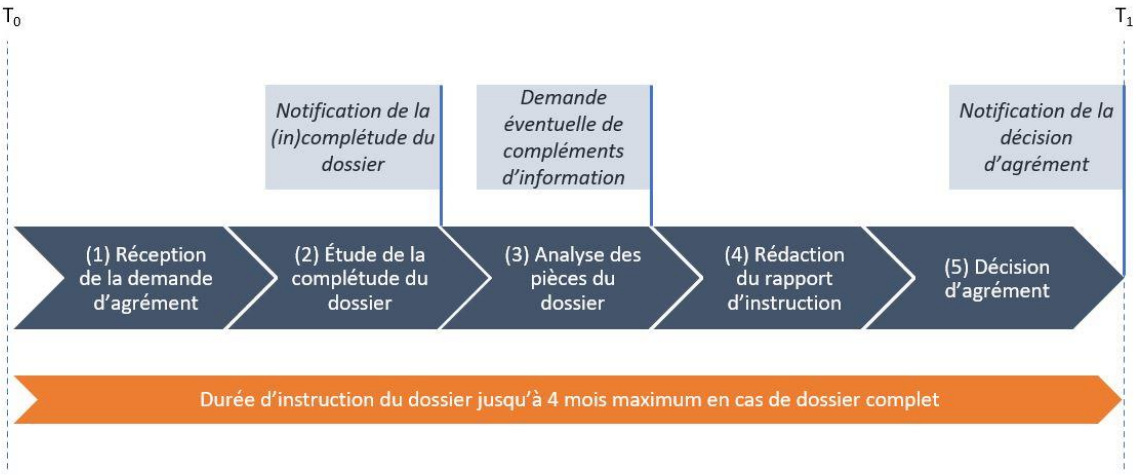
1. la liste des procédures d'exploitation utilisées, qui est structurée par thématique. La thématique sécurité doit être explicitée. Elle doit couvrir notamment :
    a. procédures de gestion des journaux ;
    b. procédures de gestion des alertes ;
    c. procédures de mise à jour régulière de tous les composants (systèmes d'exploitation, applications, routeurs, etc.) ;
    d. procédures de gestion des composants à mise à jour fréquente (anti-virus, systèmes de détection d'intrusion le cas échéant) ;
    e. procédures de mise à jour en cas d'édition d'un correctif de sécurité critique ;
    f. Procédures pour la mise en sécurité des systèmes en cas d'urgence ou de danger imminent ;
    g. procédures d'exploitation des composants du SI (serveurs, routeurs) ;
    h. procédures d'exploitation des comptes et mots de passe ;
    i. procédures de gestion des composants infogérés ;
    j. procédures relatives à la sécurité physique (gardiennage, etc.) ;
    k. procédures de gestion des sauvegardes et des restaurations ;
    l. procédures pour la télé-administration ;
2. la documentation décrivant les procédures listées supra est communiquée. Afin de faciliter l'analyse, la liste supra inclut la référence précise (document, section, page) de chaque procédure dans la documentation.

[E_AGR_PRO3] Le chapitre « niveaux de service (SLA) » décrit les éléments suivants :

1. la liste des niveaux de service (SLA) mis en place tant en interne qu'en externe vis-à-vis des fournisseurs, classés par typologie (réseau, sécurité, disponibilité applicative, …) ;
2. pour chaque SLA, la liste précise la description de l'indicateur, la méthode de calcul, son ou ses seuils, son caractère interne ou externe, le délai maximum d'intervention, les pénalités en cas de non-respect.

V Procédure d'agrément d'un opérateur de jeux

Le schéma ci-dessous présente les différentes étapes de l'instruction d'une demande d'agrément.



V.1 Contenu du dossier

Le volet SI du dossier de demande d'agrément d'un opérateur de jeu déposé auprès de l'ANJ, dans un format dématérialisé, comprend les pièces définies dans l'exigence **[E_AGR_DOS1]** (cf IV).

[E_AGR_PDA1] Il appartient à l'opérateur de jeux de s'assurer, le cas échéant, que l'entreprise qui met à sa disposition une plateforme ou un logiciel communique à l'ANJ l'ensemble des éléments nécessaires à l'instruction de la demande.

[E_AGR_PDA2] L'absence d'une pièce exigée dans un dossier de demande d'agrément doit être dûment justifiée. A défaut, le dossier est réputé incomplet.

[R_AGR_PDA3] En cas de doute, il est recommandé de consulter l'ANJ préalablement au dépôt de toute demande d'agrément afin notamment d'éviter la suspension de l'instruction du dossier, pour des raisons d'incomplétude du dossier notamment.

V.2 Modalités de transmission des livrables

[E_AGR_TRF1] Le dossier de demande d'agrément est à remettre à l'ANJ par le biais du canal d'échange sécurisé mis à disposition des candidats à l'agrément. Un échange préalable est requis pour ce faire où le candidat précise les noms, prénoms et adresses de courriel de ses agents habilités à déposer tout ou partie du dossier.

S'agissant du SMA, lorsqu'il est déjà mis en place, l'envoi des codes sources sur support physique de type clé USB reste toutefois envisageable exceptionnellement, auquel cas, les codes sources devront être chiffrés et transmis selon la procédure que l'ANJ aura indiquée à l'opérateur.

V.3 Instruction de la demande

L'ANJ dispose d'un délai de quatre mois pour instruire la demande d'agrément.

Lorsque la demande d'agrément est formée par un opérateur de jeux ou de paris en ligne, le silence gardé pendant quatre mois par l'ANJ sur cette demande vaut décision de rejet (art. 8 du décret n° 2010-482 du 12 mai 2010 modifié)

Lorsque le dossier de demande n'est pas complet, l'Autorité nationale des jeux adresse à l'entreprise candidate un courrier lui demandant d'y remédier dans un délai qui ne peut être inférieur à quinze jours. L'instruction est suspendue pendant ce délai. Si, à l'expiration du délai imparti, les informations ou pièces demandées ne sont pas parvenues à l'Autorité, la demande d'agrément est rejetée. Au cours de l'instruction, l'entreprise candidate est tenue de fournir, à la requête de l'Autorité nationale des jeux, toute information légalement justifiée et de nature à éclairer cette dernière sur des éléments contenus dans le dossier déposé.

Les décisions relatives à l'agrément sont notifiées à l'opérateur et publiées sur le site de l'ANJ.

VI Régime de l'agrément

VI.1 Cycle de vie

[E_AGR_SUA1] L'opérateur de jeu nouvellement agréé doit déposer un dossier de certification à 6 mois du SMA lors de sa mise en œuvre initiale, conformément aux exigences techniques volumes 3 et 5.

[E_AGR_SUA2] L'opérateur agréé devra, pour tout jeu qu'il souhaite offrir, déposer un dossier d'homologation logicielle, conformément aux exigences techniques volume 2 et obtenir une décision favorable avant la fourniture du service aux joueurs.

[E_AGR_SUA3] L'opérateur agréé doit ouvrir un service de jeu au plus tard un an après l'obtention de l'agrément, sauf accord explicite contraire formalisé avec l'Autorité.

[E_AGR_SUA4] l'opérateur agréé est tenu d'assurer et maintenir la sécurité et la robustesse de son système d'information dans l'ensemble de ses composantes, conformément aux exigences techniques dans leur ensemble. Il est donc attendu de l'opérateur qu'il mette en œuvre l'ensemble des mesures permettant de répondre à cet objectif, en termes de mises à jour techniques, de structures et processus organisationnels et de mécanismes de contrôle adaptés.

[E_AGR_SUA5] L'opérateur agréé doit chaque année, à la date anniversaire d'obtention de son agrément, déposer auprès de l'autorité un dossier de certification conformément aux exigences techniques volume 5.

VII Annexes

VII.1 Annexe n°1 : glossaire traverse au corpus des exigences techniques

Le lecteur est invité à consulter le fichier nommé :

Glossaire transverse au corpus des exigences techniques v1.0.xlsx

Une version pdf est également mise à disposition.

VII.2 Annexe n°2 : matrices de correspondance pour les livrables du volet SI de l'agrément

Le lecteur est invité à consulter le fichier nommé :

Matrices de correspondance livrables ET1 v1.0.xlsx

Une version pdf est également mise à disposition.