AUTORITÉ NATIONALE DES JEUX

FRANZÖSISCHE REPUBLIK

TECHNISCHE ANFORDERUNGEN AN DIE INFORMATIONSSYSTEME VON GLÜCKSSPIELBETREIBERN

Zusammenfassung

Gemäß Art. 34 VIII des Gesetzes von 12 zu Art. 32 des Dekrets Nr. 2010-518 in seiner ab dem 1. Oktober 2020 anwendbaren Fassung, der vorsieht, dass das Collège de l'ANJ (Französische Glücksspielbehörde) die für seine Anwendung erforderlichen technischen Anforderungen festlegt, werden in diesem Dokument die technischen Anforderungen an die Informationssysteme von Glücksspielbetreibern festgelegt.

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

Inhaltsverzeichnis

I Allgemeine Beschreibung

I.1 Rappel des obligations légales et réglementaires

Artikel L. 320-3 des Gesetzbuchs für innere Sicherheit:

„ Ziel der Glücksspielpolitik des Staates ist es, das Angebot und den Konsum von Spielen zu begrenzen und zu regulieren und deren Funktionsweise zu kontrollieren, um:

1. übermäßiges oder zwanghaftes Glücksspiel zu verhindern und Minderjährige zu schützen;

2. Integrität, Zuverlässigkeit und Transparenz des Glücksspielbetriebs zu gewährleisten;

3. betrügerische oder kriminelle Aktivitäten sowie Geldwäsche und Terrorismusfinanzierung zu verhindern;

4. ein ausgewogenes Funktionieren der verschiedenen Arten von Glücksspiel zu gewährleisten, um eine wirtschaftliche Destabilisierung der betreffenden Sektoren zu vermeiden.“

Artikel L. 320-4 des Gesetzbuchs für innere Sicherheit:

„ Die in Artikel L. 320-6 definierten Glücksspielbetreiber tragen zu den in Artikel L. 320-3 Nummern 1, 2 und 3 genannten Zielen bei. Ihr Glücksspielangebot hilft, die Nachfrage nach Glücksspielen in einem von der Behörde kontrollierten Kreislauf zu kanalisieren und die Entwicklung eines illegalen Glücksspielangebots zu verhindern.”

Art. 34 VIII des Gesetzes Nr. 2010-476 vom 12. Mai 2010 über die Öffnung für den Wettbewerb und die Regulierung des Online-Glücksspielsektors:

„ Die französische Glücksspielbehörde legt die technischen Merkmale von Online-Glücksspiel- und Wettplattformen und -software für Betreiber, die einer Lizenzierungsregelung unterliegen, und Betreiber mit ausschließlichen Rechten fest. Sie bewertet das Sicherheitsniveau regelmäßig.

Sie legt die technischen Anforderungen an die Integrität des Glücksspielbetriebs und die Sicherheit von Informationssystemen fest, die die Betreiber einhalten müssen. Sie legt die technischen Parameter von Online-Glücksspielen zur Anwendung der in den Artikeln 13 und 14 dieses Gesetzes vorgesehenen Dekrete fest. […]

Sie bewertet die von den Betreibern eingeführten internen Kontrollen. Zu diesem Zweck kann sie eine Prüfung von Informationssystemen oder -prozessen durchführen oder verlangen. […]”
Dekret vom 27. März 2015 zur Genehmigung der für Online-Glücksspielbetreiber geltenden Spezifikationen (Anhang, Artikel 11).

I.2 Présentation du corpus des exigences techniques

Um die Lesbarkeit und Umsetzung der verschiedenen Kategorien von technischen Anforderungen zu erleichtern, wurde einerseits die Entscheidung getroffen, sie vollständig neu zu schreiben, um das Regelwerk anzupassen, und sie andererseits in fünf Bände aufzuteilen, um ihre Aneignung durch die Glücksspielbetreiber zu erleichtern.

1. **Band 1: Technische Anforderungen an die Lizenzierung und Sicherheit von Informationssystemen**

In diesem Band werden die architektonischen und materiellen Verpflichtungen sowie die organisatorischen, informations- und verfahrenstechnischen Verpflichtungen in Bezug auf die Sicherheitspolitik von Informationssystemen zusammengefasst.

Ziel ist es, die technischen und personellen Ressourcen zu bewerten, die zur Bewältigung der Risiken im Zusammenhang mit technischen und funktionalen Systemen für die Datenerhebung, -verwaltung und -speicherung verwendet werden.

Diese Anforderungen müssen vom Betreiber umgesetzt werden, sobald die Lizenz eingeholt ist und die Präsentation ihrer Umsetzung den technischen Teil der Anweisung des Antrags auf Verlängerung der Lizenz untermauert. Ohne förmliche Genehmigung muss der Teil des Informationssystems für Betreiber mit ausschließlichen Rechten für Glücksspiele, die unter diese ausschließlichen Rechte fallen, konzeptionell dieselben Anforderungen enthalten, soweit sich die hier dargelegten Anforderungen auf das gesamte Informationssystem oder funktionsübergreifende Komponenten beziehen.

Dieser Band, der sich umfassend mit dem Informationssystem auseinandersetzt und mit der Reife der Organisation in Bezug auf Sicherheit verbunden ist, erhält seine volle Bedeutung erst in Verbindung mit den anderen Bänden

2. **Band 2: Technische Anforderungen an die Softwarezertifizierung**

Dieses Dokument legt den Rahmen für die Genehmigung von Glücksspiel- und Wettsoftware fest, um die Integrität und Sicherheit von Spielsoftware zu gewährleisten.

Es definiert den Umfang der Genehmigung, ihren technischen Umfang und die Einzelheiten des Verfahrens, wobei die von den Betreibern erwarteten Dokumente und Informationen formalisiert und strukturiert werden.

3. **Band 3: Technische Anforderungen an die Bereitstellung von Daten gemäß Art. 31 und 38 des Gesetzes Nr. 2010-476 vom 12. Mai 2010**

Dieser Band ermöglicht die Festlegung der Mechanismen, die eingerichtet werden müssen, um die Integrität und Kohärenz der Aufzeichnung von Glücksspieldaten, die Verfahren für die Bereitstellung und den Formalismus der Aufzeichnungen über das physische Speichermedium (PSM) zu gewährleisten.

Ferner sollen die Informationen festgelegt werden, die die Betreiber über das PSM jederzeit zur Verfügung stellen müssen, damit die Behörde ihre Aufgabe, die Tätigkeit der Glücksspielbetreiber ständig zu überwachen, wahrnehmen kann (Art. 31 und 38 des Gesetzes Nr. 2010-476 vom 12. Mai 2010).

4. Band 4: Technische Anforderungen für die Abfrage der Glücksspielverbotsdatei

In diesem Band werden die technischen Verfahren (Bildung von Abfrageschlüsseln, Kanälen und Konsultationsmechanismen von DNS-Diensten) festgelegt, die von den Betreibern zur Abfrage der Glücksspielverbotsdatei gemäß Artikel 22 des Dekrets Nr. 2010-518 vom 19. Mai 2010 in der geänderten Fassung umzusetzen sind.

Dieser Band sieht nicht die Verwaltung der Datei durch die Behörde vor.

5. Band 5: Technische Anforderungen an die Zertifizierung

Dieser Abschnitt enthält alle technischen Anforderungen an die Architektur und Sicherheitsmaßnahmen, die von den Zertifizierungsstellen im Zusammenhang mit der Zertifizierung des PSM sechs Monate nach Beginn der Tätigkeit zu prüfen sind, und die jährliche Zertifizierung gemäß Artikel 23 des geänderten Gesetzes Nr. 2010-476 vom 12. Mai 2010, um sicherzustellen, dass ein angemessenes Niveau der Systemsicherheit aufrechterhalten wird.

Die Bände 1 bis 5 gelten für die gesamte Tätigkeit des Betreibers.

I.3 Présentation et objectifs du document

Gemäß Art. 34 VIII des Gesetzes Nr. 2010-476 vom 12. Mai 2010 über die Öffnung für den Wettbewerb und die Regulierung des Online-Glücksspielsektors, in der geänderten Fassung, legt die ANJ die technischen Merkmale von Plattformen und Software für Online-Glücksspiele und Wetten von Betreibern fest, die einer Lizenzierungsregelung unterliegen oder die Inhaber von Ausschließlichkeitsrechten sind.

Zu diesem Zweck enthält dieses Dokument die technischen Anforderungen für den Lizenzantrag, der den Markteintritt eines Betreibers markiert und dann nach fünf Jahren abläuft, wenn die Lizenz erneuert wird. Aber die Anforderungen sind als technische, sicherheitstechnische und organisatorische Anforderungen zu verstehen, die für alle Betreiber unbedingt dauerhaft sein müssen.

Das Lizenzierungsverfahren für Glücksspielbetreiber muss es der Behörde ermöglichen, Folgendes zu gewährleisten:

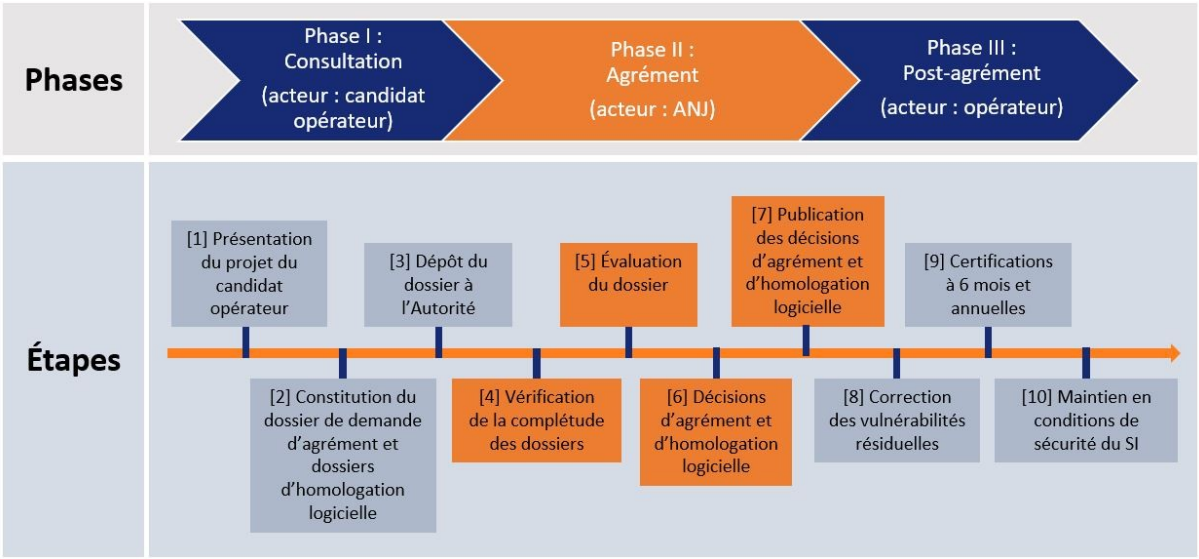
- Einhaltung der PSM-Regeln. Im Falle eines neuen Betreibers, für den das PSM noch nicht vorhanden wäre, besteht die Herausforderung darin, sicherzustellen, dass seine Umsetzungsstrategie die PSM-Anforderungen berücksichtigt;
- die langfristige Sicherheit und Robustheit des Informationssystems, sowohl in seinen technischen als auch in organisatorischen Komponenten, auf denen die Spiele und die damit verbundenen Dienste (Spielerkontodienste, Zahlungen, Glücksspielbetrieb usw.) vom Betreiber umgesetzt werden.

Die von der Behörde in diesem Zusammenhang ergriffenen Maßnahmen sind Teil des Kontrollsystems, das sie eingerichtet hat, um die in Artikel L. 320-3 des Gesetzbuchs für innere Sicherheit festgelegten Ziele zu erreichen. Wenn die Bewertung eines Lizenzantrags zeigt, dass die eingesetzten Ressourcen die Erfüllung dieser Ziele nicht ermöglichen, wird die ANJ den Lizenzantrag ablehnen. Insbesondere ergibt sich aus Art. 21 III Unterabs. 1 des geänderten Gesetzes vom 12. Mai 2010, dass die Behörde die Erteilung oder Verlängerung einer Lizenz „*wegen der technischen Unfähigkeit (…) des Antragstellers, den Verpflichtungen im Zusammenhang mit seiner Tätigkeit oder dem Schutz der öffentlichen Ordnung, der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung, den Erfordernissen der öffentlichen Sicherheit, und der Bekämpfung übermäßiger oder pathologischer Glücksspiele nachhaltig nachzukommen*“ verweigern kann.

Das Dokument enthält:

- Anwendungsbereich des Lizenzierungsverfahrens, d. h. in welchen Fällen der Betreiber eine Lizenz beantragen muss (Abschnitt II);
- Anwendungsbereich der Lizenz für die IS-Komponente in ihren Grundsätzen (Abschnitt III);
- Inhalt des Lizenzdossiers für die IS-Komponente, d. h. die Dokumente, aus denen sie besteht, und die Anforderungen für jedes dieser Dokumente hinsichtlich des Inhalts und der Organisation der angeforderten Informationen (Abschnitt IV)
- das Lizenzierungsverfahren (Abschnitt V);
- Folgemaßnahmen zur Lizenz (Abschnitt VI).

Die verschiedenen Phasen des Lizenzierungsverfahrens sind in der nachstehenden Abbildung dargestellt:



Phases	Phasen
Étapes	Stufen
Phase I : Consultation (acteur : candidat opérateur)	Phase I: Konsultation (Akteur: antragstellender Betreiber)
Phase II : Agrément (acteur : ANJ)	Phase II: Lizenz (Akteur: ANJ)
Phase III : Post-agrément (acteur :	Phase III: Nachlizenzierung (Akteur:

opérateur)	Betreiber)
[1] Présentation du projet du candidat opérateur	[1] Vorstellung des Vorhabens des antragstellenden Betreibers
[2] Constitution du dossier de demande d'agrément et dossiers d'homologation logicielle	[2] Konstitution des Lizenzantrags und der Softwarezertifizierungsdossiers
[3] Dépôt du dossier à l'Autorité	[3] Einreichung des Dossiers bei der Behörde
[4] Vérification de la complétude des dossiers	[4] Überprüfung der Vollständigkeit der Dossiers
[5] Évaluation du dossier	[5] Auswertung des Dossiers
[6] Décisions d'agrément et d'homologation logicielle	[6] Software-Genehmigungs- und Lizenzierungsentscheidungen
[7] Publication des décisions d'agrément et d'homologation logicielle	[7] Veröffentlichung von Software-Genehmigungs- und Lizenzierungsentscheidungen
[8] Correction des vulnérabilités résiduelles	[8] Korrektur von verbleibenden Schwachstellen
[9] Certifications à 6 mois et annuelles	[9] 6-Monats- und Jahreszertifizierungen
[10] Maintien en conditions de sécurité du SI	[10] Aufrechterhaltung des IS unter sicheren Bedingungen

I.4 Glossaire

Dieses Glossar deckt alle technischen Anforderungen der Bände 1 bis 5 ab. Jeder Band reproduziert identisch die Elemente des Glossars mit dem einzigen Ziel, die Arbeit der Leser zu erleichtern, indem ihnen ein autarkes Dokument zur Verfügung gestellt wird.

DSGVO: Allgemeine Datenschutzverordnung

Cloud: „Cloud-Computing-Dienst“: ein digitaler Dienst, der den Zugang zu einem flexiblen und variablen Satz von IT-Ressourcen ermöglicht, die gemeinsam genutzt werden können;

Vertraulichkeit: Die Eigenschaft, dass die Informationen nicht an unbefugte Personen, Organisationen oder Prozesse zur Verfügung gestellt oder weitergegeben werden.

Cyber-Risiko: Cyber-Risiko bezieht sich auf jede Verletzung von Computer- und Kommunikationssystemen sowie von gespeicherten oder übertragenen Daten. Diese Vorfälle, die wahrscheinlich das Funktionieren der Organisation blockieren, können durch bösartige Handlungen, unbeabsichtigte menschliche Fehler oder technische Störungen verursacht werden.

Verfügbarkeit: die Eigenschaft, auf Anfrage durch eine autorisierte Einrichtung zugänglich und verwendbar zu sein.

Management von Vorfällen: alle Verfahren, die für die Erkennung, Analyse und Eindämmung eines Vorfalls relevant sind, sowie alle Verfahren und Protokolle, die für die Reaktion auf den Vorfall relevant sind.

Vorfall: jedes Ereignis, das sich wirklich negativ auf die Sicherheit von Informationssystemen und -netzen auswirkt.

Integrität: Die vollständige und unveränderte Natur von Informationen, die beweisen, dass sie seit ihrer Validierung keiner Ergänzung, Entnahme oder zufälligen oder vorsätzlichen Änderung unterzogen wurden.

Spielplattform: Das Computersystem des Betreibers, das einer Spielaktivität gewidmet ist. Dieses besteht hauptsächlich aus Hardware- und Software-Ressourcen, die insbesondere die vollständige Verwaltung des Glücksspielbetriebs ermöglichen.

Risiko: eine Kombination aus Bedrohung und Verlusten, die sie verursachen kann, d. h. die Angemessenheit der Ausnutzung einer oder mehrerer Schwachstellen einer oder mehrerer Entitäten durch ein bedrohliches Element, das eine Angriffsmethode mit Auswirkungen auf die wesentlichen Elemente und die Organisation verwendet.

Restrisiko: das Risiko bleibt nach dem Risikomanagementverfahren bestehen.

IT-System: ein IT-System repräsentiert alle Hardware- und Softwareressourcen, die organisiert sind, um Informationen zu sammeln, zu speichern, zu verarbeiten und zu kommunizieren.

Informationssystemsicherheit (ISS): die Sicherheit eines Informationssystems beinhaltet die Verringerung der Risiken für das Informationssystem, um deren Auswirkungen auf den Betrieb und die Geschäftstätigkeit von Unternehmen zu begrenzen.

Rückverfolgbarkeit: Eine Eigenschaft, die Nichtabstreitbarkeit ermöglicht und Rechenschaftspflicht gewährleistet. Das heißt, dass diese Eigenschaft den Ursprung der Quelle, den Bestimmungsort, die Richtigkeit einer Maßnahme und die Identifizierung der verantwortlichen Einrichtung garantiert.

Authentizität: Die Art der Informationen (Dokument, Daten), die nachweislich echt ist, von der Person, die behauptet, sie erstellt oder erhalten zu haben, tatsächlich erstellt oder erhalten wurde und zum angegebenen Zeitpunkt erstellt oder erhalten wurde.

Sensor: ein Bestandteil des Sammlungs- und Archivierungssystems, dessen Funktion darin besteht, Spuren zu erstellen. Die Spuren-Erstellungsfunktion entspricht der Formatierung der Daten, die zwischen dem Spieler und der Spielplattform zirkulieren, und der anschließenden Übermittlung dieser an das Tresormodul des Erfassungs- und Archivierungssystems.

Tresor: ein konstituierendes Element des PSM, dessen Funktion darin besteht, die vom Spieler stammenden oder von der Spielplattform bereitgestellten Daten zu verschlüsseln, zu signieren, mit einem Zeitstempel zu versehen und zu archivieren. Dies dient dazu, Vertraulichkeit, Authentizität und Vollständigkeit im Laufe der Zeit zu gewährleisten.

Physisches Speichermedium (PSM): ein Gerät zum Sammeln und Speichern von Daten, die zwischen dem Spieler und der Glücksspielplattform des Betreibers während des Glücksspielbetriebs ausgetauscht werden. Dieses Gerät ist unter der Verantwortung des Betreibers zu entwickeln und zu betreiben.

ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information (Nationale Agentur für Cybersicherheit Frankreichs).

CNIL: Commission Nationale de l'Informatique et des Libertés (Französische Datenschutzbehörde).

Sicherheitsanforderung: Sicherheitseigenschaft für Informationen, Prozesse, Dienstleistungen oder materielle Vermögenswerte (Beispiele: Verfügbarkeit, Integrität, Vertraulichkeit).

Sicherheitsrichtlinie: Anwendung der ISSP auf ein bestimmtes Thema.

Sensible Daten: Im Sinne dieser Anforderungen handelt es sich bei sensiblen Daten um nicht als Verschlusssachen eingestufte Informationen oder Materialien, die, wenn sie der Öffentlichkeit zugänglich gemacht werden (über jegliche Kommunikationsmittel, an den Berufskreis, ohne dass sie es wissen müssen, oder im Zusammenhang mit dem persönlichen Umfeld) oder wenn ein Dokument gefälscht wurde, das Image oder die Interessen der ANJ, der Betreiber, die Inhaber einer Genehmigung oder eines ausschließlichen Rechts sind, der Organisationen, die vertraglich oder durch Vereinbarung gebunden sind, oder deren Personals schädigen könnten.

z. B.: Prüfberichte (Zulassung, Zertifizierung, Lizenz usw.), Quellcodes, Genehmigungsbericht, Anweisungsberichte, Aktionsplan usw.

Sensibles Dokument: Ein sensibles Dokument ist ein Dokument, das Personen (auch intern) nicht zur Kenntnis gebracht werden darf, die es nicht kennen müssen.

Gefürchtetes Ereignis: ein Vorfall, der die Verfügbarkeit, Integrität und/oder Vertraulichkeit von Informationen, Prozessen, Dienstleistungen oder materiellen Vermögenswerten beeinträchtigt (z. B.: Nichtverfügbarkeit des Dateiservers).

Schweregrad: Schätzung des Ausmaßes und der Intensität der Auswirkungen eines Risikos. Der Schweregrad ist ein Maß für wahrgenommene negative Auswirkungen, sei es direkt oder indirekt.

Sicherheitsgenehmigung: Validierung durch eine Genehmigungsbehörde, dass das von der Organisation erzielte Sicherheitsniveau den Erwartungen entspricht und dass die Restrisiken im Rahmen der Studie akzeptiert werden.

Zertifizierung: Analyse, die es einem Kunden ermöglicht, durch den Einsatz eines kompetenten und kontrollierten unabhängigen Fachmanns, der als Zertifizierungsstelle bezeichnet wird, sicherzustellen, dass ein Produkt eine oder mehrere Normen erfüllt.

Sicherheitsvorfall: ein Ereignis oder eine Reihe von Ereignissen, die sich auf die Verfügbarkeit, Integrität und/oder Vertraulichkeit von Informationen, Prozessen, Dienstleistungen oder materiellen Vermögenswerten auswirken.

Bedrohung: ein Oberbegriff für jede feindselige Absicht, Schaden anzurichten.

Sicherheitsmaßnahme: Mittel des Umgangs mit einem Risiko in Form von Lösungen oder Anforderungen, die in einen Vertrag aufgenommen werden können. Eine Maßnahme kann funktional, technisch oder organisatorisch sein. Sie kann sich auf Informationen, einen Prozess, einen Dienst, einen materiellen Vermögenswert, einen Interessenträger im Ökosystem auswirken.

Interessenträger: eine Person, Personengruppe, Organisation oder Risikoquelle in direkter oder indirekter Interaktion mit dem Studiengegenstand (Beispiele: ein Dienstleister, der an einem IS-System arbeitet, ein Lieferant).

Business Continuity Plan (BCP): eine formalisierte Reihe von Verfahren und Maßnahmen, die sicherstellen sollen, dass die Geschäftstätigkeit ohne Unterbrechung fortgesetzt wird, und um die Verfügbarkeit von Informationen unabhängig von den aufgetretenen Vorfällen sicherzustellen.

Notfallwiederherstellungsplan (DRP): eine formalisierte Reihe von Verfahren zur Wiederherstellung und Reaktivierung eines Informationssystems im Falle einer Katastrophe oder eines größeren Vorfalls, der zu einer Betriebsunterbrechung führt (Beispiele: Brand, Ausfall usw.).

Informationssystemsicherheitspolitik (ISSP): eine formalisierte Reihe strategischer Elemente, Richtlinien, Verfahren, Verhaltenskodizes, organisatorischer und technischer Vorschriften mit dem Ziel, das Informationssystem(en) zu schützen.

Sicherheitsgrundsatz: Die Sicherheitsgrundsätze sind Ausdruck der notwendigen Sicherheitsrichtlinien und der wichtigen Merkmale der ISS für die Entwicklung einer ISSP.

Sensible Stelle: eine Stelle im Personalbereich, die direkten oder indirekten Zugriff auf personenbezogene Daten im Sinne der DSGVO, oder das Glücksspielbetrieb oder sensible Daten haben kann.

Sicherheitsregel: Sicherheitsregeln definieren die Mittel und Verhaltensweisen im Rahmen der ISSP. Sie werden durch die Anwendung von Sicherheitsprinzipien in einem bestimmten Umfeld und Kontext geschaffen.

Risiko: Szenario, das ein gefürchtetes Ereignis und alle Bedrohungen beschreibt, die es möglich machen. Sein Niveau wird in Bezug auf Schwere und Wahrscheinlichkeit geschätzt.

Anfangsrisiko: Risikoszenario, das vor der Anwendung der Risikobehandlungsstrategie bewertet wurde. Sein Niveau wird in Bezug auf Schwere und Wahrscheinlichkeit geschätzt.

Restrisiko: Risikoszenario, das nach Anwendung der Risikobehandlungsstrategie verbleibt. Sein Niveau wird in Bezug auf Schwere und Wahrscheinlichkeit geschätzt.

Software as a Service (SaaS): ein Software-Geschäftsmodell, in dem ein Drittanbieter Softwareanwendungen hostet und seinen Kunden über Online-Dienste zur Verfügung stellt.

Risikoquelle: ein Element, eine Person, eine Gruppe von Personen oder eine Organisation, die ein Risiko verursachen könnte, versehentlich oder absichtlich.

Informationssystem (IS): Die strukturierten technischen Ressourcen (Computerhardware, Netzwerkausrüstung, Software, Geschäftsprozesse und -verfahren) und sozialen Ressourcen (Organisationsstruktur und IS-bezogene Personen) bei einer Organisation, die auf die Entwicklung, Aufzeichnung, Verarbeitung, Einordnung, Speicherung und Verbreitung von Informationen ausgerichtet sind.

Das Informationssystem darf nicht mit dem IT-System verwechselt werden, das nur eine Untergruppe des ersten ist.

IT-System: alle für die Verarbeitung von Informationen erforderlichen IT-Ressourcen (Computer, Programme, Netzwerk, Software usw.).

Wahrscheinlichkeit: Schätzung der Wahrscheinlichkeit eines Risikos.

ANJ: Autorité Nationale des Jeux (Französische Glücksspielbehörde).

Online-Glücksspiel und Wetten: Glücksspiele und Wetten, bei denen die Verpflichtung über einen öffentlichen Online-Kommunikationsdienst eingegangen wird.

Spielregeln: eine Reihe von Normen, die die Bedingungen regeln, unter denen ein Spiel gespielt wird. Die Spielregeln beschreiben unter anderem die erforderliche Ausrüstung für das Spiel, die Anzahl der erlaubten Spieler, den Zweck des Spiels (oder die Bedingungen des Sieges), die Startsituation des Spiels und wie man das Spiel spielt.

Spielmechanik (oder Spiellogik): in diesem Dokument verstanden als alle Berechnungen, die Verarbeitung von Informationen und die Verhaltensweisen, die die Umsetzung der Spielregeln ermöglichen, die das Spiel definieren.

Primitiv (des Spiels): elementare Spielinformationsverarbeitungsfunktion. Die Sequenz eines kohärenten Satzes von Spielprimitiven zielt darauf ab, Spielmechaniken zu schaffen.

Business-Funktionen (im Sinne von Spielsoftware): eine Reihe von Spielprimitiven und Funktionen, die zur Implementierung von Spielmechaniken und Regeln beitragen, die ein Spiel definieren.

Software-Architektur: Organisation der verschiedenen Komponenten eines Softwarepakets.

Informationssystem (IS): Die strukturierten technischen Ressourcen (Computerhardware, Netzwerkausrüstung, Software, Geschäftsprozesse und -verfahren) und sozialen Ressourcen (Organisationsstruktur und IS-bezogene Personen) bei einer Organisation, die auf die Entwicklung, Aufzeichnung, Verarbeitung, Einordnung, Speicherung und Verbreitung von Informationen ausgerichtet sind.

Spielplattform: alle technischen Infrastrukturen, die zum Zweck der Bereitstellung von Glücksspieldiensten für Spieler oder Wetter implementiert wurden.

Infrastruktur- oder Serviceelemente können vom Betreiber oder von Dritten selbst verwaltet werden (Beispiele: Hosting durch Dritte, Infrastruktur von Drittanbietern, Spielsoftwarelösung, die von einem Dritten bereitgestellt wird).

Spielsoftware: alle Computeranwendungen oder Programme, die die Spielmechanik implementieren.

Alle Computeranwendungen oder Programme, die die Spiellogik ganz oder teilweise unterstützen oder verändern, gelten als integraler Bestandteil der Spielsoftware.

Die Spielsoftware besteht konzeptionell aus folgenden Geschäftskomponenten:

- Einem in die Spielplattform integrierten Spiel-Engine;
- Einem Totalisator für gemeinsame Wettspiele;
- Einem Zufallsgenerator für Glücksspiele;

- Einem oder mehreren Spiel-Clients, die den Spielern zur Verfügung stehen (Beispiele: Web-Anwendung, mobile Anwendungen für Android und iOS, Terminal-Software, Verkaufsstellenterminal-Software, automatische Remote-Gaming-Systeme;
- API[1]-Diensten, die in die Spielplattform integriert sind, ermöglichen es den verschiedenen Anwendungskomponenten der Spielplattform oder einer anderen externen Anwendung (einschließlich Spiel-Clients), mit der Spiel-Engine zu interagieren.

Wenn die Spielsoftware nach modularer Architektur entwickelt wurde, die die oben beschriebene Aufschlüsselung in Geschäftskomponenten berücksichtigt, kann die Software-Genehmigung modular verarbeitet werden.

Spiel-Engine: eine Komponente der Gaming-Software, die normalerweise in die Spielplattform integriert ist und für die Bereitstellung von Gaming-Primitiven für die Spielsoftware oder sogar für die vollständige Verwaltung des Glücksspielbetriebs verantwortlich ist (Beispiele: Wetten im Sport und Pferderennen, Ziehen und Handeln von Karten im Poker, Berechnung und Verteilung von Gewinnen usw.). Der Vorteil eines Spiel-Engines, der als separates Modul entwickelt wurde, liegt in der Modularität der Lösung und der Abstraktionsschicht, die sie für die Entwicklung von Spielen bietet, die darauf basieren. Die Spielregeln und Mechaniken werden in der Regel von der Spiel-Engine angetrieben.

Totalisator (für gegenseitige Wetten): eine Komponente der gegenseitigen Glücksspielsoftware, die normalerweise in die Spiel-Engine integriert ist und eine Reihe von Berechnungen als Teil eines Spiels macht, wie die Berechnung der Einsätze, der Auszahlungsquoten der gewinnenden Spiele und der Gewinncoupons der Spieler.

Spiel-Client: eine Komponente der Spielsoftware, die Spielern oder Wettern oder sogar Verkaufsstellen-Händlern zur Verfügung gestellt wird, die es diesen ermöglichen, in einer „Client-Server"-Beziehung mit der Spielplattform, insbesondere mit der Spiel-Engine, zu interagieren (Beispiele: Konsultation des vom Betreiber angezeigten Glücksspielangebots, Platzierung von Wetten, Konsultation der Wettergebnisse und der damit verbundenen Gewinne).

Der Spiel-Client kann die gesamte oder einen Teil der Spielmechanik implementieren und in verschiedenen Formen erhältlich sein:

- Webanwendung, die über einen Webbrowser von der Website des Betreibers aus zugänglich ist;
- Computeranwendung in Form eines Fat Clients, der auf dem Arbeitsplatz des Benutzers installiert werden soll;
- Anwendung für mobile Geräte oder Tablets;
- Antrag auf Verkaufsstellen-Terminals;
- Automatisches System zur Abwicklung von Glücksspielen aus der Ferne (z. B.: Software für Wetten per SMS oder Instant Messaging).

[1] API: Anwendungsprogrammierschnittstelle. Lösung, die es Anwendungen ermöglicht, miteinander zu kommunizieren und Dienste oder Daten auszutauschen, *via* eine Programmiersprache.

Es ist zu beachten, dass sich der Spiel-Client konzeptionell von dem verwendeten Anwendungsclient unterscheidet. Zum Beispiel enthält der Anwendungsclient im Falle einer Mobiltelefonanwendung den Spiel-Client, kann aber auch Dienste wie Kontoverwaltung, Spielstatistiken, Nachrichten usw. enthalten. Die Genehmigung des Spiel-Clients ist nicht dazu bestimmt, diese Nebendienste abzudecken, aber sie ist notwendig, sicherzustellen, dass der Spiel-Client in Bezug auf die Sicherheit ordnungsgemäß isoliert ist.

(Automatisches) Terminal, auch bekannt als Gaming-Terminal ohne menschliche Vermittlung: ein Hardwaregerät, das in einem physischen Vertriebsnetz positioniert ist (Beispiele: Rennbahnen, Einzelhändler, Tabakhändler), das eine Spiel-Client-Software-Schnittstelle enthält, die direkt für Spieler oder Wetter zugänglich ist. Dieses Gerät ermöglicht es, das Spiel zu spielen, die Ergebnisse eines Spiels und die damit verbundenen Gewinne zu konsultieren. Es autorisiert auch Zahlungsvorgänge (Einlagen und Auszahlung von Geld) unter Bedingungen, die zuvor den Spielern mitgeteilt wurden.

Verkaufsstellen-Terminal, auch bekannt als Gaming-Terminal mit menschlicher Vermittlung: Der Verkaufsstellen-Terminal hat die gleichen Funktionen wie die Verkaufsstellen-Station, jedoch ist der Zugriff auf die Softwareschnittstelle auf das vom Betreiber autorisierte Personal und den Verkaufsstellenmanager beschränkt (Beispiele: Einzelhändler, Tabakhändler). Das Terminal kann über Managementfunktionen für Einzelhändler verfügen (Bestandsverwaltung, Buchhaltung, Ticketverkauf usw.).

Internet-Terminal: die Möglichkeit des Spielers, auf das Internet zuzugreifen. Dies ist in der Regel ein Computer, kann aber auch ein Telefon oder ein Tablet sein, vorausgesetzt, das Medium gibt dem Spieler direkten Zugriff auf die Website.

Zufallszahlengenerator (RNG): ein Gerät, das in der Lage ist, eine Abfolge von Werten mit zufälligen (oder nahezu zufälligen) Eigenschaften zu erzeugen, für die es schwierig, wenn nicht gar unmöglich ist, Zahlengruppen zu identifizieren, die identifizierbaren Vorhersageregeln folgen.

Dieses Gerät wird implementiert, wenn der Verlauf des Spiels die Generierung eines zufälligen Elements erfordert, zum Beispiel im Poker mit der zufälligen Ziehung von Karten oder sogar Online-Lottospielen ohne physische Ziehung.

I.5 Identification des exigences et recommandations dans le document

Dieses Dokument enthält zwei Ebenen von Empfehlungen:

- Die Maßnahmen, denen **[E_numero]** vorausgeht, sind **obligatorische** Anforderungen, vorbehaltlich der in diesen technischen Anforderungen genannten Ausnahmen;
- Die Maßnahmen, denen **[R_numero]** vorausgeht, sind Empfehlungen, bei denen Betreiber beschließen können, sie nicht zu befolgen, sofern sie der Behörde dies rechtfertigen und sie über die von ihnen beabsichtigten Alternativmaßnahmen unterrichten.

II Anwendungsbereich der Lizenz

Die folgenden Anforderungen beziehen sich auf die Fälle, in denen eine Lizenz erforderlich ist:

[E_AGR_CHA1] Ein neuer Betreiber wird systematisch vor einer Software-Genehmigungsentscheidung genehmigt, die jeder Eröffnung eines Spielangebots vorausgehen muss.

[E_AGR_CHA2] Ein Betreiber mit einer Lizenz muss sie am Ende ihrer fünfjährigen Gültigkeit verlängern. Das Erneuerungsverfahren ist strikt identisch mit dem ursprünglichen Verfahren. In dem der Behörde vorgelegten Dossier wird angegeben, welche Elemente sich fünf Jahre zuvor gegenüber der Situation geändert haben.

III Umfang der IS-Komponente der Lizenz

[E_AGR_PER1] Der Geltungsbereich der IS-Komponente der Lizenz erstreckt sich auf alle organisatorischen und technischen Aspekte des IS des Betreibers, wie er implementiert (Fall einer Verlängerung der Lizenz) oder zu implementieren ist (Fall einer neuen Lizenz), wobei ein besonderer Schwerpunkt auf den spezifischen Komponenten im Zusammenhang mit Glücksspielen (Spielerkonto, Sensor, PSM usw.) und der Sicherheit des IS als Ganzes liegt.

IV Inhalt des Lizenzdossiers für die IS-Komponente

IV.1 Liste des documents exigés et dispositions communes

[E_AGR_DOS2] Das bei der ANJ eingereichte Lizenzantragsdossier eines Glücksspielbetreibers in einem dematerialisierten Format enthält die folgenden Dokumente:

1. den Masterplan des Informationssystems;
2. die Sicherheitspolitik der Informationssysteme;
3. ein Rahmendokument, das eine umfassende und detaillierte Architektur beschreibt. Diesem Dokument sind folgende Anlagen beizufügen:
    a. ein Anhang mit dem PSM (Sensor und Tresor);
    b. einen Anhang mit dem Tool für die Verwaltung des Spielerkontos und den Zugriffskanälen für den Spieler;
    c. einen Anhang mit IS-Plattformen und Lieferantentools;
    d. einen Anhang, in der die Prozesse und das Serviceniveau (SLA) aufgeführt sind;

Die Bestimmungen über jedes der oben aufgeführten Dokumente, insbesondere den erwarteten Inhalt, sind in den folgenden Abschnitten aufgeführt.

[E_AGR_DOS2] Mit Ausnahme eines neuen Betreibers, der die Infrastruktur und die Prozesse noch nicht vollständig umgesetzt hat, müssen die verschiedenen Dokumente die aktuelle Situation zum Zeitpunkt der Einreichung widerspiegeln, insbesondere die ISSP und der Masterplan müssen der aktuellen Fassung entsprechen.

Der Betreiber wird darauf hingewiesen, dass die Nichteinhaltung dieser Verpflichtung **[E_AGR_DOS2]** ein Grund für die Ablehnung des Lizenzantrags ist.

[E_AGR_DOS3] Für den Fall, dass bestimmte Abschnitte der Dokumente nur die Prognose enthalten, ohne dass die Arbeiten abgeschlossen sind, von einem neuen Betreiber, der noch nicht seine gesamte Infrastruktur und Prozesse eingerichtet hat, muss er:

1. den Zeitplan für das Ausfüllen dieser Unterlagen in das Lizenzantragsdossier aufnehmen;
2. der Behörde die zusätzlichen Informationen gemäß dem mitgeteilten Zeitplan übermitteln;
3. und diese Elemente beim Zertifizierer zur Analyse bei der nächsten Zertifizierung einreichen.

Dies, sofern die fraglichen Abwesenheiten keine Unvollständigkeit des Dossiers darstellen, die seine Prüfung behindert, was von der Behörde zu beurteilen ist.

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

[E_AGR_DIR1] Der Masterplan des Informationssystems folgt dem nachstehenden detaillierten Plan:

1. Unternehmensstrategie nach 3-5 Jahren;
2. Informationssystemstrategie;
3. Organisation der Funktion des Informationssystems;
4. Humanressourcen der Funktion des Informationssystems;
5. Haushaltsmittel;
6. IS-Verwaltung.

Das Dokument kann zusätzliche Abschnitte enthalten, wenn der Betreiber oder Prüfer dies für erforderlich hält.

Für den Fall, dass die anwendbaren Dokumente den für die oben genannten Kapitel angeforderten Inhalten entsprechen, muss der Lizenzbewerber eine Korrespondenzmatrix zwischen dem oben beschriebenen Plan und den spezifischen Abschnitten und der Paginierung des Dokuments/der Dokumente bereitstellen.

[E_AGR_DIR2] Das Kapitel „Unternehmensstrategie" beschreibt folgendes:

1. Das Datum der Erstellung des Masterplans, der abgedeckte Zeitraum und die geplanten Aktualisierungstermine sind anzugeben.
2. Die Unternehmensstrategie über einen Zeitraum von drei bis fünf Jahren, in dem Kontext, Ambitionen und Positionierung dargestellt werden;
3. geschäftliche Herausforderungen, die mit diesem Ziel verbunden sind.

[E_AGR_DIR3] Das Kapitel „Informationssystemstrategie" beschreibt folgendes:

1. IT-Leitlinien, die den gesamten Anwendungsbereich des IS abdecken;
2. Strukturierende IS-Projekte, die den geschäftlichen Herausforderungen entsprechen, sowie ihr detailliertes Ziel, mögliche Phasen und ihren Zeitplan. Die ISS-Komponente in jedem Projekt sollte erläutert werden.
3. Für die eingeleiteten Projekte ist eine Zusammenfassung der bisherigen Fortschritte beigefügt.

[E_AGR_DIR4] Das Kapitel „Organisation der Funktion des Informationssystems“ enthält mindestens Folgendes:

1. die verschiedenen Strukturen, aus denen es besteht, mit ihren spezifischen Aufgaben;
2. alle verbundenen Einrichtungen mit ihren jeweiligen Funktionen und geografischen Standorten;

[E_AGR_DIR5] Das Kapitel „Humanressourcen der Funktion des Informationssystems“ enthält mindestens Folgendes:

1. die entsprechende Anzahl des internen Personals und Vollzeitäquivalente (VZÄ) nach Strukturen und Aufgaben der Informationssystemfunktion werden spezifiziert, wobei zumindest zwischen den Funktionen Betrieb, Informationssystemsicherheit, Infrastrukturprojekte, Anwendungsprojekte und MCO, Management und Strategie unterschieden wird;
2. gegebenenfalls Änderungen der Personalprognose über den Zeitrahmen des Masterplans;
3. die auf die Funktion des Informationssystems anwendbare Outsourcing-Politik;
4. darin sind die Unternehmen oder Aufgaben im Zusammenhang mit der Vergabe oder Auslagerung von Unteraufträgen (insbesondere Webhosting, Facility Management, Sicherheit usw.) und die entsprechenden Volumina (VZÄ) festgelegt.

[E_AGR_DIR6] Das Kapitel „Haushaltsmittel“ enthält mindestens Folgendes:

1. den jährlichen Gesamthaushalt des IS über den Zeitrahmen des Masterplans;
2. geschätzte Verteilung nach wichtigen Bereichen (Betriebsfunktion, Informationssystemsicherheit, Infrastrukturprojekte, Anwendungsprojekte und MCO) aufgeschlüsselt nach Jahren über den Zeitraum des Masterplans;
3. seine projizierte jährliche Verteilung über die Zeitskala des Masterplans durch Strukturierung von IS-Projekten, die die IS-Strategie widerspiegeln.

[E_AGR_DIR7] Das Kapitel „IS-Verwaltung“ beschreibt folgendes:

1. Die Akteure, die an der IS-Verwaltung beteiligt sind, ihre jeweiligen Rollen und Verantwortlichkeiten.
2. Die für die Verwaltung des IS-Projektportfolios eingerichtete Komitologie, darunter insbesondere die im Kapitel „Informationssystemstrategie“ genannten Strukturierungsprojekte.

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

[E_AGR_SSI1] Die Informationssystemsicherheitspolitik (ISSP) folgt dem nachstehenden detaillierten Plan:

1. Politik, Organisation, Verwaltung;
2. Humanressourcen;
3. Vermögensverwaltung;
4. Integration der Sicherheit von Informationssystemen in den Lebenszyklus von Projekten;
5. Physische Sicherheit;

6. Netzwerksicherheit;
7. Architektur von Informationssystemen;
8. Betrieb von Informationssystemen;
9. Sicherheit des Arbeitsplatzes;
10. Sicherheit der Systementwicklung;
11. Umgang mit Vorfällen;
12. Geschäftskontinuität;
13. Konformität, Audit, Kontrolle

Das Dokument kann zusätzliche Abschnitte enthalten, wenn der Betreiber oder Prüfer dies für erforderlich hält.

Für den Fall, dass die anwendbaren Dokumente den für die oben genannten Kapitel angeforderten Inhalten entsprechen, muss der Lizenzbewerber eine Korrespondenzmatrix zwischen dem oben beschriebenen Plan und den spezifischen Abschnitten und der Paginierung des Dokuments/der Dokumente bereitstellen.

[E_AGR_SSI2] Detaillierte technische Untergliederungen der in ihrer Sicherheitspolitik erforderlichen Elemente sind mit ihrer Verknüpfung zur ISSP versehen, einschließlich der Verfahren im Zusammenhang mit Informationssystemen sowie der (organisatorischen und technischen) Mittel zur Gewährleistung der Sicherheit und ihrer Überwachung im Laufe der Zeit.

[E_AGR_SSI3] Das Kapitel „Politik, Organisation, Verwaltung“ beschreibt:

- Das Datum des Beginns der Anwendung der Sicherheitspolitik der Informationssysteme;
- Die regelmäßige Aktualisierung der Sicherheitspolitik der Informationssysteme;
- Die strategischen Ausrichtungen und den Umfang der Umsetzung der sich daraus ergebenden Maßnahmen;
- Den Anwendungsbereich der Sicherheitspolitik der Informationssysteme;
- Die rechtlichen und regulatorischen Aspekte im Zusammenhang mit dem Anwendungsbereich der Sicherheitspolitik;
- Den Umfang der Anforderungen, der eine Gewichtung und Referenzwerte gemäß den gewählten Sicherheitskriterien und eine Liste der durch Beispiele gestützten Auswirkungen enthält;
- Eine Beschreibung der Sicherheitsanforderungen der Tätigkeitsbereiche des Betreibers im Einklang mit dem im vorherigen Abschnitt dargelegten Umfang der Anforderungen;
- Analyse der für den Umfang der Studie ausgewählten und nicht ausgewählten Bedrohungen mit Begründungen;
- Eine Beschreibung der Organisation, die zur Gewährleistung der Sicherheit der Informationssysteme und der physischen Sicherheit der Räumlichkeiten eingerichtet wurde;
  Das Vorhandensein der folgenden Funktionen und die angeforderten Informationen sind anzugeben:
  - Sicherheitsbeauftragter für Informationssysteme: genaue Festlegung der Zuständigkeiten, Grad der Formalisierung, Anzahl der Assistenten und Berichterstattungslinie;
  - Betriebsbehörde des Informationssystems (IS) (oder gleichwertige Funktion): genaue Festlegung der Zuständigkeiten, Grad der Formalisierung und gegebenenfalls Art der Zuständigkeiten für die Informationssystemsicherheit (ISS);

    - Spezialisierter ISS-Anwalt: Nummer und Berichterstattungslinie;
    - Interne ISS-Auditoren: Nummer und Berichterstattungslinie;
    - Interne Kontrollfunktion der ISS: Nummer und Berichterstattungslinie;
    - ISS-Unterstützungsfunktion: Nummer und Berichterstattungslinie;
    - ISS-Betriebsfunktion: Nummer und Berichterstattungslinie);
    - ISS-Designfunktion: Nummer und Berichterstattungslinie;
- ISS-Dashboard-Modelle;

[E_AGR_SSI4] Das Kapitel „Humanressourcen“ beschreibt den Anteil des Personals des Betreibers, das in der ISS, in den IS- und ISS-Ketten sowie unter den Nutzern sensibilisiert oder geschult wurde. Darüber hinaus legt es fest, ob die Kompetenz aller regelmäßig verwaltet und überwacht wird.

[E_AGR_SSI5] Das Kapitel „Vermögensverwaltung“ beschreibt die Verfahren und Mechanismen zum Schutz der vom Betreiber verarbeiteten Daten, insbesondere:

- Personenbezogene Daten seiner Kunden;
- Daten und Statistiken über das Spiel oder bestimmte Spieler, deren Kenntnis einem Spieler einen Vorteil verschaffen könnte;
- „Geheime“ Spieldaten (z. B. Karten anderer Spieler oder Karten, die in einem Pokerspiel nicht umgedreht wurden).
- Die Verfahren zur Identifizierung und Klassifizierung sensibler Komponenten (einschließlich Daten) und die damit verbundene Methodik;

[E_AGR_SSI6] Das Kapitel „Integration der ISS in den Projektlebenszyklus“ beschreibt:

- Das Sicherheitsmanagement, das der Betreiber in jeder Phase des Systementwicklungszyklus implementiert, in den Phasen der Definition, Entwicklung, des Betriebs und der Nutzung, dann der Wartung und Entwicklung. Der Betreiber legt seine Politik im Falle einer festgestellten Schwachstelle und des Fehlens von Abhilfemaßnahmen dar;
- Das ISS-Annahmeverfahren für Informationssystemprojekte, bevor sie in Betrieb genommen werden, und Angabe des Anteils der Informationssysteme, die tatsächlich Gegenstand einer solchen Abnahme waren;
- Die Verfahren für die Durchführung einer formalisierten Prüfung der Auswirkungen auf die IS-Sicherheit oder die Inbetriebnahme einer neuen Komponente (Servermodell, Betriebssystem, Anwendung, Daten usw.) ;
- Durchgeführte Risikostudien. Die Methodik wird spezifiziert;
- Kontrollen von Unterauftragnehmern, um sicherzustellen, dass das Sicherheitsniveau ihrer Plattformen und Informationssysteme aufrechterhalten wird.

[E_AGR_SSI7] Das Kapitel „Physische Sicherheit“ beschreibt:

- Die Verfahren zur Überprüfung von Bewerbern, die sich um eine sensible Stelle bewerben;
- Verfahren zur Bewältigung von Interessenkonflikten;
- Verfahren zum Schutz von Informationen, wenn Personal das Unternehmen verlässt;
- Sicherheitsmaßnahmen für sein Personal;
- Die zum Schutz der technischen Räumlichkeiten eingesetzten Mittel;
- Durchgeführte Brandschutzmaßnahmen;

- Die Redundanzpolitik der Stromversorgung;
- Die H24-Überwachungspolitik seiner Betriebsstätten;
- Physische Zugangsverwaltungspolitik;

[E_AGR_SSI8] Das Kapitel „Netzwerksicherheit“ beschreibt:

1. Betriebs- und Überwachungszentren für Computer und Netzwerke: ihren Standort, ihre gehosteten Anwendungen und ihr zugewiesenes Personal;
2. Hosting-Zentren: Standort und Art des Hostings;
3. Verbindungszentren: die Arten der verwendeten Verbindungen;
4. Operative Zentren;
    a. Für Spielplattformen, Front-End und alle damit verbundenen Informationssysteme muss der Lizenzantragsteller Folgendes angeben:
    b. Die ausgeführte(n) Funktion(en);
    c. Die Art der verarbeiteten Daten;
    d. Die Gesellschaft oder Behörde, die für ihren Betrieb verantwortlich ist;
    e. Den Zugangsanbieter;
    f. Den Hosting-Dienstleister.
5. Die angewendete Netzwerkpartitionierung
6. Die Netzwerkfilterpolitik und die Beschreibung der Filterregeln in Bezug auf Weißlisten.
7. Die verwendeten Arten der Netzwerkpartitionierung (IP-Filterung, Anwendungsfilterung, VLAN, 802. 1X, NAP/NAC, etc.).
8. Die zur Abwehr von konventionellen IP-Angriffen eingeführten Sicherheitsmechanismen und zugehörigen Protokolle, insbesondere im Zusammenhang mit Netzwerk-Denial-of-Service-Angriffen;
9. Technische und organisatorische Maßnahmen zur Netzwiderstandsfähigkeit seiner Informationssysteme, insbesondere zur Bekämpfung von Denial-of-Service-Angriffen (verteilt oder anderweitig durch Erschöpfung der Bandbreite oder der Systemressourcen) auf der Ebene der Glücksspielplattformen und des Front-Ends: Der Betreiber beschreibt insbesondere die technischen Prozesse (Lastausgleich, DNS-TTL-Anpassung, dynamische IP-Umadressierung von Plattformen und Front-End) und die damit verbundenen organisatorischen Maßnahmen (Alerting im Falle eines Angriffs, Absichtserklärung mit ISPs zur Bekämpfung von DDOS usw.).

[E_AGR_SSI9] Das Kapitel „IS-Architektur“ beschreibt alle Mechanismen und Maßnahmen, die umgesetzt werden, um die Vertraulichkeit und Integrität der Abläufe innerhalb seiner Glücksspielplattformen und Front-End-Plattformen zu gewährleisten: Diese Ströme betreffen Administratoren, die Teil des Personals des Betreibers sind, wie Betreiber, externe Administratoren wie diejenigen, die Fernwartungen von Ausrüstungen durchführen usw.

[E_AGR_SSI10] Der „Betrieb des IS“ beschreibt:

1. Spieleridentifikations- und Authentifizierungsmechanismen;
2. Zugangskontrollmechanismen der Spieler: Einzelheiten zu etwaigen Spielerprofilen und Mechanismen zur Aufteilung von Rechten;
3. Kryptografische Prozesse zur Gewährleistung der Authentifizierung von Komponenten, Vertraulichkeit und Authentizität der folgenden Mitteilungen:
    a. Kommunikation zwischen dem Betreiber und der ANJ;

b. Netzkommunikation zwischen den Akteuren und dem Betreiber;
c. Netzwerkkommunikation zwischen Modulen innerhalb des Front-Ends;

4. Eine Beschreibung aller Mechanismen und Maßnahmen, die zur Gewährleistung der Vertraulichkeit und Integrität der Ströme innerhalb ihrer Glücksspielplattformen und des Front-Ends durchgeführt werden: Diese Ströme betreffen Administratoren, die Teil des Personals des Betreibers sind, wie Betreiber, externe Administratoren wie diejenigen, die Fernwartungen von Ausrüstungen durchführen usw.;
5. Eine Beschreibung der Mechanismen für den Zugang zu den Verwaltungsfunktionen der Glücksspielplattform und des Front-Ends einschließlich;
6. Die Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus bei der Verwaltung von Authentifizierungsgeheimnissen (insbesondere robuste Passwörter, regelmäßige Änderungen, starke Authentifizierung) für das Bedienpersonal des Betreibers;
7. Das Verfahren zur Anwendung von Patches, insbesondere im Falle einer Regression;
8. Die technischen Verfahren für den Fall, dass ein Patch zu einer möglichen Regression führen würde;
9. Beschreibung der Protokollierung von Warnungen und wie lange sie gespeichert werden.

[E_AGR_SSI11] Das Kapitel „ Sicherheit des Arbeitsplatzes“ beschreibt:

1. Das Verfahren für die Bereitstellung und die Verwaltung von Arbeitsplätzen;
2. Das formalisierte Verfahren für die Konfiguration von Arbeitsplätzen;
3. Physische Schutzmechanismen gegen Diebstahl;
4. Verwaltung von Berechtigungen auf Arbeitsplätzen;
5. Verwaltung des Zugangs bei Nomadentum wie Telearbeit;
6. Verwaltung von Wechselspeichermedien.

[E_AGR_SSI12] Das Kapitel „Sicherheit der Systementwicklung“ beschreibt:

1. Die Mittel, die der Betreiber verwendet, um die persönlichen Daten und die Privatsphäre der Spieler zu schützen;
2. Kontrollmaßnahmen und -methoden zur Bewertung der Entwicklungen in jeder Phase eines Entwicklungsprojekts;
3. Den sicheren Entwicklungsrahmen für Projekte, bei denen der Betreiber für die Entwicklung verantwortlich ist;

Der Betreiber teilt die Verträge mit seinen Dienstleistern in Bezug auf die Umsetzung eines sicheren Entwicklungsrahmens für die von ihm ausgelagerten Projekte mit.

[E_AGR_SSI13] Das Kapitel „Umgang mit Vorfällen“ beschreibt:

1. Die Betriebsart des Betriebszentrums, das für die ISS des Betreibers zuständig ist. Es legt insbesondere die Berichterstattung, das Bereitschaftssystem und das ständige Personal fest. Andernfalls legt es die Verfahren für die Überwachung und Auslösung von Warnmeldungen fest;
2. Verfahren zur Bewältigung von Vorfällen und Betrugsaufdeckung. Es legt den Umfang der Verbreitung dieser Dokumente und die vorgesehenen Warnverfahren fest.
3. Den Status von ISS-Vorfällen oder Betrugsfällen, die der Betreiber möglicherweise festgestellt hat. Es legt die Vorkommnisse (insbesondere die Ermittlung der Eingangsquellen und -ebenen) und die vorgenommene Verwaltung fest;

4. Die implementierten Lösungen zur Verhinderung oder gegebenenfalls zur Erkennung von Angriffen und Eindringen auf seine Informationssysteme.

[E_AGR_SSI14] Das Kapitel „Geschäftskontinuität“ beschreibt:

1. Den Archivierungsdienst zur Sicherstellung der Speicherung aller seiner Verarbeitungsdaten, insbesondere der im Front-End-Tresor gespeicherten Daten. Der Betreiber gibt die Art der Medien und das Sicherungsformat an,
2. Die Archivierungsmechanismen und die sicheren Mittel zum Schutz der Archive, die der Betreiber implementieren kann;
3. Die Modalitäten seines Sicherungsplans. Der Betreiber legt insbesondere die Verfahren und Fristen für die Wiederherstellung einer Sicherung nach einem Vorfall sowie den/die Ort(e), an dem/denen die Sicherungen gespeichert werden, und die für diesen/diese Standort(e) angewandten Sicherheitsmaßnahmen fest.
4. Die Pläne für die Geschäftskontinuität und die Notfallwiederherstellungspläne, die der Betreiber im Rahmen seiner Geschäftstätigkeit erstellen konnte, und die Verfahren, die er zur Anpassung an den Front-End-Kontext vorsieht.

[E_AGR_SSI15] Das Kapitel „Konformität, Audit, Inspektion, Kontrolle“ beschreibt die Art, die Periodizität, die Akteure und die Methodik der ISS-Audits, die an Informationssystemen und Anwendungen durchgeführt werden. Der Betreiber teilt die Berichte und die wichtigsten Empfehlungen mit. Es legt fest, wie Abhilfemaßnahmen zu beschließen, durchzuführen und zu überwachen sind. Darin ist der Anteil der tatsächlich angewandten Maßnahmen anzugeben.

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

[E_AGR_ARC1] das Dokument, das die Gesamt- und Detailarchitektur des IS beschreibt, wird dem nachstehenden detaillierten Plan folgen:

1. Die allgemeine Beschreibung der Plattform des Informationssystems:
   a. Alle im IS implementierten Komponenten und für jede die von ihr ausgeführte(n) Funktion(en);
   b. Die Art des Hostings jeder Komponente;
   c. Alle Verbindungen zwischen den Komponenten und für jede Komponente eine Beschreibung ihres Zwecks, sodass festgelegt wird, wie die Komponenten zusammenarbeiten, um das allgemeine Funktionieren des Systems zu gewährleisten;
   d. Das Unternehmen oder die Behörde, die für den Betrieb jeder Komponente verantwortlich ist.
   e. Computer- und Netzbetriebs- und Überwachungszentren mit Angabe ihres Standorts/ihrer Standorte, Betriebsmethoden und einer Schätzung der Zahl der eingeführten VZÄ;
   f. Hosting-Zentren (Standort, Art des Hostings);
   g. Verbindungszentren (Typen, Lieferanten);
   h. Operative Zentren (einschließlich Sicherheitszentrum, Kundendienstzentrum, Entwicklungsdienstzentrum usw.);

i. Netzzugangsanbieter für jede ausgehende/eingehende IS-Verbindung;
j. Ferner wird die Liste der wichtigsten Softwareanwendungen festgelegt, die im Rahmen der Tätigkeiten im Zusammenhang mit den betreffenden Lizenzen oder Tätigkeiten implementiert werden.

2. Die Gesamtdarstellung der Architektur mit logischen und physischen Netzwerkdiagrammen, Anwendungsdiagrammen, Netzwerkzuordnung;
3. Die Bestimmungen über den Anhang mit dem PSM (siehe Kapitel unten);
4. Die Bestimmungen über den Anhang mit dem Tool für die Verwaltung des Spielerkontos und den Zugangskanälen für den Spieler (siehe Kapitel unten);
5. Die Bestimmungen über den Anhang mit IS-Plattformen und Lieferantentools (siehe Kapitel unten).

Das Dokument kann zusätzliche Abschnitte enthalten, wenn der Betreiber oder Prüfer dies für erforderlich hält.

Für den Fall, dass die anwendbaren Dokumente den für die oben genannten Kapitel angeforderten Inhalten entsprechen, muss der Lizenzbewerber eine Korrespondenzmatrix zwischen dem oben beschriebenen Plan und den spezifischen Abschnitten und der Paginierung des Dokuments/der Dokumente bereitstellen.

IV.5 Dispositions relatives au document annexe présentant le SMA

[E_AGR_SMA1] Zum Zeitpunkt der Einreichung des Lizenzantragsdossiers ist das PSM nicht unbedingt in Betrieb. Das Unternehmen muss jedoch in der Lage sein, seine detaillierte Implementierungsstrategie für die Erfassung und Sicherung aller Daten, zu dessen Sammlung sie verwendet wird, zu präsentieren.

[E_AGR_SMA2] Dazu stellt das Unternehmen ein Dokument zur Beschreibung des PSM zur Verfügung. Dieses Dokument wird dem unten beschriebenen Plan folgen und kann zusätzliche Abschnitte enthalten, wenn das Unternehmen dies für notwendig hält:

1. Allgemeine Beschreibung des PSM;
2. Detaillierte Beschreibung des Sensors für die Spurenerstellung;
3. Detaillierte Beschreibung des Tresors zur sicheren Aufbewahrung von Spuren;
4. Beschreibung der vom PSM erfassten Spurenzugangsfunktionen;
5. Besondere Bestimmungen in Bezug auf das Front-End der Glücksspielplattform;
6. Technische Anhänge.

Das Dokument kann zusätzliche Abschnitte enthalten, wenn der Betreiber oder Prüfer dies für erforderlich hält.

Für den Fall, dass die anwendbaren Dokumente den für die oben genannten Kapitel angeforderten Inhalten entsprechen, muss der Lizenzbewerber eine Korrespondenzmatrix zwischen dem oben beschriebenen Plan und den spezifischen Abschnitten und der Paginierung des Dokuments/der Dokumente bereitstellen.

[E_AGR_SMA3] Das Kapitel „Allgemeine Beschreibung des PSM (Tresor und Sensor)“ enthält die folgenden Abschnitte:

1. Die angewandte Gesamtstrategie: Dies beinhaltet die Darstellung des durchgeführten oder geplanten allgemeinen Vorgangs im Hinblick auf die sichere Sammlung und Lagerung von Spuren;

2. Die allgemeine Architektur, in der die verschiedenen Komponenten des PSM, ihre Rolle, ihre Positionierung in Bezug auf die Spielplattform und ihre Interaktionen mit der Spielplattform, den Spielern und allen anderen möglichen IS dargestellt werden;

[E_AGR_SMA4] Das Kapitel „Detaillierte Beschreibung des **Sensors**“ enthält die folgenden Abschnitte:

Allgemeiner Rahmen:

1. Die detaillierte Strategie für den Sensor in Bezug auf die Generierung von Spuren. Dies beinhaltet die Darstellung der ausgewählten Sensorlösung und des zugehörigen Betriebs gegenüber den ausgetauschten Daten, deren Spuren erforderlich sind (Beispiel: Wahl eines Sensors, der den Anwendungsfluss zwischen dem Spieler und der Spielplattform für Abfragen des Spielers unterbricht);

2. Die in Bezug auf die geforderte sehr hohe Verfügbarkeit verwendete Strategie, in der die im Falle der Nichtverfügbarkeit oder Störung des Sensors durchgeführten Maßnahmen festgelegt werden;

3. Die am Sensor durchgeführte Risikoanalyse;

4. Die anwendbare Sicherheitspolitik, einschließlich einer detaillierten Beschreibung der Sicherheitsmaßnahmen für Sensoren;

5. Der Sensor im logischen Sinne kann aus mehreren physikalischen Sensoren bestehen, die möglicherweise von unterschiedlicher Art sind. Die angeforderte Beschreibung muss für jeden verwendeten physikalischen Sensor angegeben werden.

Durchführung:

6. Identität und Kontaktdaten des/der Dienstleister(s), der/die für die Entwicklung und Wartung des Sensors oder des Anbieters der ausgewählten Sensorlösung verantwortlich sind;

7. Die detaillierten Spezifikationen des Sensors einschließlich:

    a) Die detaillierte funktionale und technische Architektur (Anwendung und Netzwerk) des Sensors;

    b) Die Spezifikationen der Schnittstellen und gegebenenfalls der vom Sensor implementierten „Proxy“-Funktionen (Anwendungsfluss);

    c) Die Beschreibung der verschiedenen Ströme (d. h. Datentyp, Protokolle), die den Sensor durchlaufen;

    d) Eine detaillierte Beschreibung der Mechanismen zur (positiven oder negativen) Anerkennung von Spuren durch die Spielplattform und den Tresor;

e) Eine detaillierte Beschreibung der Mechanismen für die Batch-Verarbeitung von Spuren in Bezug auf die Übermittlung von Spuren an den Tresor;

f) Eine detaillierte Beschreibung der im Rahmen des Datenaustauschs eingerichteten Authentifizierungs- und Vertraulichkeitsmechanismen:

- Zwischen dem Spieler und dem Sensor;
- Zwischen dem Sensor und der Spielplattform;

8. Wenn das PSM bereits umgesetzt ist, die Liste und die Ergebnisse der durchgeführten Audittests;

Hosting:

9. Die physikalische Position des Sensors;
10. Wie der Sensor gehostet wird;
11. Identität und Kontaktdaten des Dienstleisters, der den Sensor hostet;
12. Die Erstellung des Hosting-Vertrags/der Hosting-Verträge;
13. Dokumente über die Verwaltung und den Betrieb des Sensors;
14. Die Verfahren, die insbesondere im Hinblick auf den Schutz vor unbefugtem Zugriff angewandt werden;

[E_AGR_SMA5] Das Kapitel „Detaillierte Beschreibung des **Tresors**“ enthält die folgenden Abschnitte:

Allgemeiner Rahmen:

1. Die detaillierte Strategie zur sicheren Aufbewahrung von Spuren. Dies beinhaltet die Präsentation der gewählten Tresorlösung und der damit verbundenen Funktionsweise;
2. Die im Hinblick auf die geforderte sehr hohe Verfügbarkeit verwendete Strategie, in der die im Falle der Nichtverfügbarkeit des Tresors durchgeführten Maßnahmen festgelegt werden;
3. Die am Tresor durchgeführte Risikoanalyse;
4. Die anwendbare Sicherheitspolitik, einschließlich einer detaillierten Beschreibung der Sicherheitsmaßnahmen im Tresor;

Durchführung:

5. Identität und Kontaktdaten des/der Dienstleister(s), der/die für die Entwicklung und Wartung des Tresors verantwortlich ist/sind, oder des Lieferanten der ausgewählten Tresorlösung;
6. Die detaillierten Spezifikationen des Tresors, einschließlich:

a) Die detaillierte funktionale und technische Architektur des Tresors;

b) Eine detaillierte Beschreibung der für den Datenaustausch eingerichteten Authentifizierungs- und Vertraulichkeitsmechanismen:

- Zwischen dem Sensor und dem Tresor;

- Zwischen dem Tresor und dem ANJ-Informationssystem;

c) Beschreibung der verschiedenen Algorithmen zur sicheren Speicherung von Spuren (Beispiel: Spurenverkettung);

7. Wenn das PSM bereits umgesetzt ist, die Liste und die Ergebnisse der Berichte über durchgeführte Tests;

Hosting:

8. Der physische Standort des Tresors (dieser muss gemäß Art. 31 des Gesetzes Nr. 2010-476 vom 12. Mai 2010 in der französischen Metropole eingerichtet sein);
9. Wie der Tresor gehostet wird;
10. Identität und Kontaktdaten des Dienstleisters, der den Tresor hostet;
11. Die Erstellung des Hosting-Vertrags/der Hosting-Verträge;
12. Dokumente über die Verwaltung und den Betrieb des Tresors, insbesondere:
    a) Der genaue Ablauf der geplanten Zeremonie der Initialisierung des Tresors und der Übergabe der erforderlichen Schlüssel;
    b) Spezifikation und Rolle der verwendeten Schlüsselpaare;
    c) Detaillierte Beschreibung der Mechanismen für die Authentifizierung natürlicher Personen für den Zugang zum Tresor;
    d) Eine detaillierte Beschreibung der Verwaltungs- und Managementfunktionen der Tresornutzer;
13. Die Verfahren, die insbesondere im Hinblick auf den Schutz vor unbefugtem Zugriff angewandt werden;

[E_AGR_SMA6] Das Kapitel „Beschreibung der vom PSM erfassten Spurenzugangsfunktionen“ enthält die folgenden Abschnitte:

1. Eine detaillierte Beschreibung des Tools für die Fernabfrage und das Sammeln von Spurendateien, einschließlich:
    a) Detaillierte funktionale und technische Spezifikationen;
    b) Wenn das PSM bereits umgesetzt ist, die Berichte über die durchgeführten Tests;
2. Eine detaillierte Beschreibung des Tools für die Validierung und Extraktion von Spurendateien, einschließlich:
    a) Detaillierte funktionale und technische Spezifikationen;
    b) Wenn das PSM bereits umgesetzt ist, die Berichte über die durchgeführten Tests;

[E_AGR_SMA7] Das Kapitel „Technische Anhänge“ enthält:

1. Wenn das PSM bereits implementiert ist:

   a) Den Quellcode des Sensors;

   Die Behörde behält sich das Recht vor, zum Zeitpunkt der Prüfung der Lizenz oder später zusätzlich Folgendes zu verlangen:

   b) Den Quellcode des Tresors;

   c) Den Quellcode des Tools für die Fernabfrage und das Sammeln von Spurendateien;

   d) Den Quellcode des Tools für die Validierung und Extraktion von Spurendateien;

2. Eine Kopie der Mindestsicherheitszertifizierung der ersten Stufe (CSPN) des PSM-Tresors (oder des Zeitplans für deren Erhalt, zusammen mit einem Vermerk des Bewertungszentrums oder Zertifizierungszentrums, in dem bestätigt wird, dass das Zertifizierungsverfahren eingeleitet wurde);

   a) Die CSPN muss mindestens die folgenden Elemente in Bezug auf Bedrohungen berücksichtigen:

      1. Die Einreichung oder Einspeisung von nicht autorisierten Aufzeichnungen;
      2. Änderung der Aufzeichnungen;
      3. Datendiebstahl;
      4. Verweigerung des Dienstes;

   b) Die CSPN muss auf der Ebene der Sicherheitsfunktionen mindestens die folgenden Elemente berücksichtigen:

      1. Starke Authentifizierung von Benutzern und Administratoren;
      2. Verschlüsselung, Signatur und Zeitstempelung von Ereignissen;
      3. Die Verkettung von Ereignissen.

[E_AGR_SMA8] Vor Aufnahme seiner Tätigkeit erklärt der lizenzierte Betreiber der ANJ, dass sein PSM in Betrieb ist.

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] das Dokument beschreibt das Spielerkontoverwaltungstool, und Zugriffskanäle, die den Spielern angeboten werden, folgen dem detaillierten Plan unten:

1. Technische Bedingungen für den Zugriff und die Registrierung auf der Website für jeden Spieler;
2. Technische Mittel zur Feststellung der Identität jedes neuen Spielers, seines Alters, seiner Anschrift und der Identifizierung des Zahlungskontos, auf das sein Vermögen übertragen wird;

3. Technische Vorkehrungen für das Sammeln und Auszahlen von Wetten und Gewinnen auf seiner Website;

Das Dokument kann zusätzliche Abschnitte enthalten, wenn der Betreiber oder Prüfer dies für erforderlich hält.

Für den Fall, dass die anwendbaren Dokumente den für die oben genannten Kapitel angeforderten Inhalten entsprechen, muss der Lizenzbewerber eine Korrespondenzmatrix zwischen dem oben beschriebenen Plan und den spezifischen Abschnitten und der Paginierung des Dokuments/der Dokumente bereitstellen.

[E_AGR_GCC2] Der Antragsteller muss den Erhalt mindestens eines Top-Level-Domainnamens mit der Endung „.fr“ durch Vorlage eines Registrierungszertifikats begründen. Er erklärt gegebenenfalls alle anderen Top-Level-Domainnamen mit der Endung „.fr“, die er für den Zugang zu seiner Online-Gaming-Website verwenden will, und legt die Dokumente vor, die die entsprechenden Registrierungen rechtfertigen.

[E_AGR_GCC3] Der Antragsteller muss die folgenden Merkmale seiner Website angeben:

1. Lageplan;
2. Warenzeichen:
3. Technische Merkmale der Website, Domainname;

Das Kapitel „Besondere Bestimmungen zum Front-End der Spielplattform“ enthält folgende Abschnitte:

1. Die detaillierte Beschreibung der eingerichteten Website „.fr“:
    a. Host;
    b. Standort;
    c. Quellcode;
    d. Sicherheitspolitik;
    e. Risikoanalyse;
    f. Bestehende Verwaltungs-, Betriebs- und Sicherheitsverfahren;
2. Die detaillierte Beschreibung der Umleitungsfunktionen für die Spielerverbindung;

[E_AGR_GCC4] Der Antragsteller legt die geplanten Spielkanäle fest, die es den Kunden ermöglichen, zu spielen: Fat Clients, native Anwendungen auf Smartphones oder Weiterleitung zu einer Website. Der Antragsteller gibt an, ob die Website Spielfunktionen anbietet. Er wird den geplanten Zeitplan für die Öffnung dieser verschiedenen Kanäle festlegen.

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

[E_AGR_PLA1] die Anlage, die die IS-Plattform des Unternehmens beschreibt, folgt für jede der Komponenten, die als Teil der Anforderung **[E_AGR_ARC1]**, beschrieben in Absatz IV.3

Bestimmungen über das Rahmendokument, in dem die umfassende und detaillierte Architektur beschrieben wird, identifiziert wurden, den unten beschriebenen Plan. Sie kann zusätzliche Abschnitte enthalten, wenn der Betreiber oder Prüfer dies für erforderlich hält:

1. Eine detaillierte Architekturbeschreibung für jede der im Rahmendokument aufgeführten IS-Komponenten gemäß der Anforderung **[E_AGR_ARC1]**;
2. Eine detaillierte Beschreibung der Netzwerkarchitektur und der zugehörigen Ströme.

Das Dokument kann zusätzliche Abschnitte enthalten, wenn der Betreiber oder Prüfer dies für erforderlich hält.

Für den Fall, dass die anwendbaren Dokumente dem für die oben genannten Kapitel angeforderten Inhalt entsprechen, muss der Lizenzbewerber eine Übereinstimmungsmatrix zwischen dem oben beschriebenen Plan und den spezifischen Abschnitten und der Paginierung des Dokuments/der Dokumente bereitstellen.

[E_AGR_PLA2] Für jeden Abschnitt ist in der Beschreibung Folgendes anzugeben:

1. Komponenten oder Teile von Komponenten, die an externe Lieferanten untervergeben werden (dies gilt auch, wenn die gesamte Plattform untervergeben wird);
2. die Gründe für diese Unterauftragsvergabe werden systematisch angegeben;
3. die vertraglichen Vereinbarungen über diese Unteraufträge werden beschrieben, insbesondere die Verpflichtungen in Bezug auf Serviceniveau, Verantwortlichkeiten und Sicherheit.

[E_AGR_PLA3] Für jeden Abschnitt werden Software-Tools oder Infrastrukturelemente, die sich im Bau befinden oder noch nicht in Betrieb sind, genauso berücksichtigt wie Komponenten, die bereits in der Produktion sind, als ob sie bereits für den für die betreffenden Lizenzen oder Tätigkeiten implementierten Umfang in Produktion wären.

[E_AGR_PLA4] Die Kapitel „Detaillierte Architekturbeschreibung“, die für jede der aufgeführten Komponenten geschrieben wurden, beschreiben:

1. Die detaillierte Beschreibung der Komponente, wobei jeder ihrer physikalischen und logischen Bestandteile für jeden einzelnen hervorzuheben ist:
    a. die ausgeführte(n) Funktion(en);
    b. die Art der verarbeiteten Daten;
    c. das benannte Unternehmen oder die Betriebsbehörde;
    d. gegebenenfalls die implementierten Verschlüsselungsmethoden;
    e. die Bedeutung ihrer Funktion (vom „Arbeitserleichterungs-Tool“ bis zum „wesentlichen Tool“),
    f. die Bedeutung ihrer Verfügbarkeit (von „keine Auswirkung“ bis „blockierende Auswirkung“ im Falle einer vollständigen oder teilweisen Systemabschaltung),
    g. die Bedeutung der Datenintegrität (von „keine Auswirkung“ bis „blockierende Auswirkung“ im Falle einer Datenänderung);
    h. die Bedeutung der Vertraulichkeit der Daten (von „keine Auswirkung“ bis „blockierende Auswirkung“ im Falle einer Datenweitergabe);
    i. die erwartete Lebensdauer.

2. eine detaillierte technische Beschreibung des Netzwerks, in der die Segmentierungs- und Filterelemente spezifiziert werden. Beschreibungen der operativen Netze, aber auch der Netze zur Unterstützung der Verwaltung und Überwachung.
    a. ein technisches Diagramm des Netzes;
    b. die Liste der verschiedenen zugehörigen Ströme;
    c. die Liste der Bereiche mit unterschiedlichen Empfindlichkeiten
        i. Typologie (Internet oder dediziertes Netzwerk usw.)
        ii. Sensitivität;
    d. die beschreibende Liste der Verbindungen zwischen diesen Bereichen (Rolle und Zweck);
    e. alle eingesetzten Technologien werden aufgelistet;
    f. die Liste der externen Verbindungen (dedizierte Leitungen, Netzverbindungen usw.) und der von außen mögliche Fernzugriff mit jeweils einer genauen Beschreibung der eingesetzten Technologien, Protokolle und Sicherheitsmaßnahmen.

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

[E_AGR_PRO1] Die Anlage zur Darstellung der Serviceprozesse und -ebenen folgt dem Plan in zwei folgenden Kapiteln:

1. Verwaltungs- und Betriebsabläufe
2. Serviceniveaus (SLA)

Das Dokument kann zusätzliche Abschnitte enthalten, wenn der Betreiber oder Prüfer dies für erforderlich hält.

Für den Fall, dass die anwendbaren Dokumente den für die oben genannten Kapitel angeforderten Inhalten entsprechen, muss der Lizenzbewerber eine Korrespondenzmatrix zwischen dem oben beschriebenen Plan und den spezifischen Abschnitten und der Paginierung des Dokuments/der Dokumente bereitstellen.

[E_AGR_PRO2] Das Kapitel „Verwaltungs- und Betriebsverfahren“ beschreibt Folgendes:

3. die Liste der verwendeten Verfahren, die nach Themen strukturiert werden. Das Thema Sicherheit muss klar erläutert werden. Es sollte insbesondere Folgendes umfassen:
    a. Protokollverwaltungsverfahren;
    b. Warnmanagementverfahren;
    c. Verfahren zur regelmäßigen Aktualisierung aller Komponenten (Betriebssysteme, Anwendungen, Router usw.) ;
    d. Verfahren für die Verwaltung von Komponenten, die häufig aktualisiert werden müssen (Antiviren-, Angriffserkennungs-Systeme, falls zutreffend);
    e. Aktualisierungsverfahren für den Fall, dass ein kritischer Sicherheitspatch ausgestellt wird,
    f. Verfahren zur Sicherung von Systemen im Falle eines Notfalls oder unmittelbar bevorstehender Gefahr;
    g. IS-Komponentenbetriebsverfahren (Server, Router);
    h. Konto- und Passwortbetriebsverfahren;
    i. Verfahren für die Verwaltung der verwalteten Komponenten;
    j. Physische Sicherheitsverfahren (Schutz usw.) ;
    k. Sicherungs- und Wiederherstellungsmanagementverfahren,
    l. Verfahren im Falle eines Sicherheitsvorfalls;
    m. Verfahren für die Fernverwaltung;
    n. Geschäftskontinuität und Wiederherstellungsverfahren (DRP und BCP).
4. eine Dokumentation, die die oben aufgeführten Verfahren beschreibt, wird bereitgestellt. Um die Analyse zu erleichtern, enthält die obige Liste die genaue Referenz (Dokument, Abschnitt, Seite) jedes Verfahrens in der Dokumentation.

[E_AGR_PRO3] Das Kapitel „Serviceniveaus und SLA“ beschreibt Folgendes:

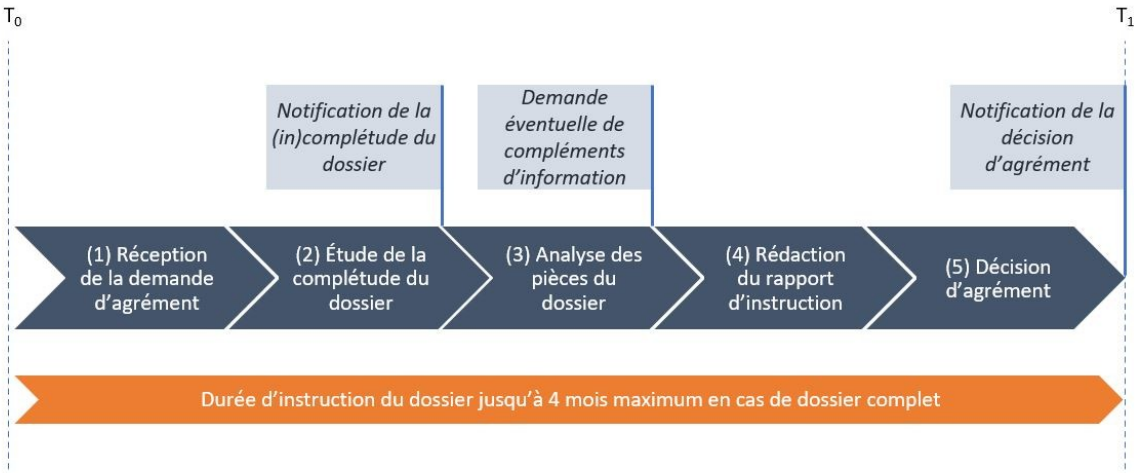
1. Die Liste der Serviceniveaus (SLA), die sowohl intern als auch extern mit Lieferanten implementiert wurden, klassifiziert nach Typ (Netzwerk, Sicherheit, Anwendungsverfügbarkeit usw.).

2. Für jede SLA sind in der Liste die Beschreibung des Indikators, die Berechnungsmethode, ihre Schwellenwerte, ihr interner oder externer Charakter sowie die maximale Interventionsfrist bei Nichteinhaltung anzugeben.

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

V Verfahren für die Lizenzierung eines Glücksspielbetreibers

Das folgende Diagramm stellt die verschiedenen Phasen der Prüfung der Lizenzanträge dar.



Notification de la (in)complétude du dossier	Benachrichtigung über (un)vollständiges Dossier
Demande éventuelle de compléments d'information	Mögliche Anfrage nach zusätzlichen Informationen
Notification de la décision d'agrément	Bekanntgabe der Lizenzierungsentscheidung
(1) Réception t de la demande d'agrément	(1) Eingang t des Lizenzantrags
(2) Étude de la complétude du dossier	(2) Prüfung der Vollständigkeit des Dossiers
(3) Analyse des pièces du dossier	(3) Analyse der Dokumente im Dossier
(4) Rédaction du rapport d'instruction	(4) Erstellung des Bewertungsberichts
(5) Décision d'agrément	(5) Lizenzierungsentscheidung
Durée d'instruction du dossier jusqu'à 4 mois maximum en cas de dossier complet	Prüfung des Dossiers bis zu maximal vier Monaten für vollständige Dossiers

V.1 Contenu du dossier

Das Lizenzantragsdossier für einen Glücksspielbetreiber, der bei der ANJ eingereicht wurde, in einem dematerialisierten Format, enthält die in der Anforderung **[E_AGR_PER2]** (siehe IV) definierten Dokumente.

[E_AGR_PDA1] Es obliegt dem Glücksspielbetreiber, gegebenenfalls sicherzustellen, dass das Unternehmen, das eine Plattform oder Software bereitstellt, der ANJ alle für die Auswertung der Anwendung erforderlichen Elemente übermittelt.

[E_AGR_PDA2] Das Fehlen eines in einem Lizenzantragsdossier erforderlichen Dokuments ist ordnungsgemäß zu begründen. Andernfalls wird das Dossier als unvollständig betrachtet.

[R_AGR_PDA3] Im Zweifelsfall wird empfohlen, vor der Einreichung eines Lizenzantrags die ANJ zu konsultieren, um insbesondere aus Gründen der Unvollständigkeit des Dossiers die Aussetzung der Dossierprüfung zu vermeiden.

V.2 Modalités de transmission des livrables

[E_AGR_TRF1] Das Lizenzantragsdossier muss der ANJ über den sicheren Austauschkanal übermittelt werden, der Lizenzbewerbern zur Verfügung gestellt wird. Zu diesem Zweck ist ein vorläufiger Austausch erforderlich, wenn der Antragsteller die Namen, Vornamen und E-Mails seiner Bevollmächtigten angibt, die befugt sind, das Dossier ganz oder teilweise einzureichen.

Im Falle des PSM, wenn es bereits vorhanden ist, bleibt das Senden der Quellcodes auf einem physischen Medium wie einem USB-Schlüssel ausnahmsweise möglich, wobei die Quellcodes nach dem Verfahren, das die ANJ dem Betreiber angegeben hat, verschlüsselt und übertragen werden müssen.

V.3 Instruction de la demande

Die ANJ hat zwei Monate Zeit, um den Lizenzantrag zu prüfen.

Wenn der Antrag auf Genehmigung von einem Online-Glücksspiel- oder Wettanbieter gestellt wird, und die ANJ vier Monate lang nichts zu diesem Antrag äußert, gilt dies als Ablehnungsentscheidung (Artikel 8 des Dekrets Nr. 2010-482 vom 12. Mai 2010 in der geänderten Fassung)

Ist das Antragsdossier nicht vollständig, übermittelt die französische Glücksspielbehörde dem antragstellenden Unternehmen innerhalb einer Frist von mindestens 15 Tagen ein Schreiben, in dem es aufgefordert wird, die Situation zu beheben. Die Untersuchung wird während dieses Zeitraums ausgesetzt. Sind die angeforderten Informationen oder Unterlagen bis zum Ablauf der Frist nicht bei der Behörde eingegangen, so wird der Lizenzantrag abgelehnt.
Im Laufe der Untersuchung ist das antragstellende Unternehmen verpflichtet, auf Antrag der französischen Glücksspielbehörde alle gesetzlich gerechtfertigten Informationen vorzulegen, die Letztere über die in dem eingereichten Dossier enthaltenen Elemente aufklären können.

Lizenzierungsentscheidungen werden dem Betreiber mitgeteilt und auf der ANJ-Website veröffentlicht.

VI Lizenzierungssystem

VI.1 Cycle de vie

[E_AGR_SUA1] Der neu lizenzierte Glücksspielbetreiber wird verpflichtet sein, bei der ersten Implementierung ein Zertifizierungsdossier nach 6 Monaten des PSM gemäß den technischen Anforderungen 3 und 5 einzureichen.

[E_AGR_SUA2] Der lizenzierte Betreiber muss für jedes Spiel, das er anbieten möchte, gemäß den technischen Anforderungen Band 2 ein Software-Genehmigungsdossier vorlegen und eine positive Entscheidung erwirken, bevor der Service den Spielern zur Verfügung gestellt wird.

[E_AGR_SUA3] Der lizenzierte Betreiber muss spätestens ein Jahr nach Erhalt der Lizenz einen Glücksspieldienst eröffnen, es sei denn, mit der Behörde wurde ausdrücklich etwas anderes vereinbart.

[E_AGR_SUA4] der lizenzierte Betreiber muss die Sicherheit und Robustheit seines Informationssystems in allen seinen Komponenten im Einklang mit den technischen Anforderungen insgesamt gewährleisten und aufrechterhalten. Daher wird erwartet, dass der Betreiber alle Maßnahmen zur Erreichung dieses Ziels in Bezug auf technische Aktualisierungen, organisatorische Strukturen und Prozesse und geeignete Kontrollmechanismen umsetzen wird.

[E_AGR_SUA5] Zum Jahrestag seiner Lizenzierung muss der lizenzierte Betreiber der Behörde jedes Jahr ein Zertifizierungsdossier gemäß den technischen Anforderungen des Bandes 5 vorlegen.

VII ANHÄNGE

VII.1 Article 12 renouvellement d'agrément

12.2.2. Informationen zur Architektur des Informationssystems.

Der Antragsteller stellt ARJEL folgende Elemente zur Verfügung:

a) Aktuelle Beschreibung der Elemente im Zusammenhang mit der allgemeinen Darstellung des Unternehmens und seiner Informationssysteme gemäß Artikel 11.4 dieser Leistungsbeschreibung in Bezug auf:

Politik und Organisation von Informationssystemen (11.4.1);

-Beschreibung von Informationssystemen (11.4.2);

-Humanressourcen für IT-Sicherheit (11.4.3);

-Pilotierung von Informationssystemen (11.4.4);

b) das Dossier der Begriffsbestimmungen gemäß Artikel 11.5.2.1 dieser Spezifikationen und in Artikel 5.7.3 Buchstabe a des Dossiers für technische Anforderungen (DET);

c) eine ANSSI-Bescheinigung, dass der Tresor Gegenstand eines Wartungsberichts im Rahmen des Zertifizierungssicherungskontinuitätsverfahrens (CSPN) der ersten Stufe oder einer CSPN-Neubewertung war;

d) Der Bericht zur Schwachstellenanalyse der Plattform gemäß Artikel 11.3.2 dieser Spezifikationen, der aus einem Bericht vom Typ „intrusives Audit" besteht, dessen Zweck darin besteht, die

Schwachstellen einer Plattform zu suchen und auszunutzen, sowie die zugehörigen Fehlerblätter, in denen die festgestellten Schwachstellen zusammengefasst werden;

e) die Liste der auf der Plattform eingesetzten Spielsoftware sowie die zugehörigen Genehmigungsnummern gemäß Artikel 11.3.1 dieser Spezifikationen.

12.3. Unterlagen, die nur im Falle einer Änderung erforderlich sind, die ARJEL nicht zur Kenntnis gebracht wird

Die in den Artikeln 12.3.1 bis 12.3.6 aufgeführten Unterlagen werden vom Antragsteller vorgelegt, wenn eine Änderung in Bezug auf sie vorgenommen wurde und sie ARJEL weder seit der Erteilung der Lizenz noch seit der letzten Zertifizierung oder seit den letzten Informationen, die den ARJEL-Diensten zur Verfügung gestellt wurden, zur Kenntnis gebracht wurde.

Das Fehlen einer Änderung wird durch eine Erklärung des Betreibers bescheinigt.