

## **APPEL D'OFFRES OUVERT**

**HEBERGEMENT DES INFRASTRUCTURES INFORMATIQUES DE  
L'AGENCE NATIONALE DE SECURITE DU MEDICAMENT ET DES  
PRODUITS DE SANTE ET PRESTATIONS ASSOCIEES.**

---

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES  
(CCTP)**

---

# SOMMAIRE

---

<b>1.</b>	<b>PRÉSENTATION DU MARCHÉ.....</b>	<b>3</b>
1.1.	PRESENTATION DE L'ANSM .....	3
1.2.	OBJET DU MARCHÉ.....	3
1.3.	DEFINITIONS .....	4
1.4.	OBJECTIFS .....	5
<b>2.</b>	<b>PRÉSENTATION DU CONTEXTE.....</b>	<b>5</b>
	PRESENTATION DU PERIMETRE SI INCLUS DANS LE MARCHÉ.....	5
<b>3.</b>	<b>PHASES DU MARCHÉ.....</b>	<b>5</b>
3.1.	PRESENTATION GENERALE DES PHASES.....	5
3.2.	DETAIL DE LA PHASE TRANSITION (REVERSIBILITE ENTRANTE) .....	6
3.3.	DETAIL DE LA PHASE DE SERVICE REGULIER.....	8
3.4.	DETAIL DE LA PHASE DE REVERSIBILITE (SORTANTE).....	8
<b>4.</b>	<b>PRESTATIONS ATTENDUES D'HÉBERGEMENT .....</b>	<b>11</b>
4.1.	INTRODUCTION.....	11
4.2.	EVOLUTION VERS DES HEBERGEMENTS CLOUD SOUVERAIN / SECNUMCLOUD.....	11
4.3.	DISPOSITIONS COMMUNES A L'ENSEMBLE DES MODULES.....	12
4.4.	SOCLE HEBERGEMENT – EXIGENCES GENERALES .....	17
4.5.	MODULE A1 – SUPPORT AUX UTILISATEURS.....	19
4.6.	MODULE A2 – FOURNITURE D'UNE CONNEXION INTERNET .....	22
4.7.	MODULE A3.1 - FOURNITURE DE CAPACITES DE TYPE INFRASTRUCTURE VIRTUELLE .....	24
4.8.	MODULE A3.2 - FOURNITURE DE SERVEURS PHYSIQUES.....	27
4.9.	MODULE A4 – SERVICE D'INFOGERANCE ET PRESTATIONS DE SERVICE ASSOCIE .....	28
4.10.	MODULE A5 – ASSISTANCE TECHNIQUE, PRESTATIONS COMPLEMENTAIRES .....	33
4.11.	MODULE A6 – PILOTAGE ET ACCOMPAGNEMENT .....	36
■	<b>LISTE RECAPITULATIVE DES ANNEXES AU PRESENT CCTP : .....</b>	<b>41</b>

## 1. PRÉSENTATION DU MARCHÉ

---

### 1.1. Présentation de l'ANSM

---

L'Agence Nationale de Sécurité du Médicament et des produits de santé (ci-après dénommée l' « ANSM », l' « Agence » ou encore le « Pouvoir Adjudicateur ») est un établissement public de l'État placé sous la tutelle du ministère chargé de la santé. L'ANSM a pour principal objectif de garantir la sécurité du médicament et des produits de santé. Elle est chargée d'évaluer les bénéfices et les risques liés à l'utilisation des produits de santé tout au long de leur vie et d'exercer la surveillance des marchés sur l'ensemble des produits de santé destinés à l'homme. Elle a pour mission d'encourager la recherche et de piloter ou coordonner les études de suivi de patients ou de recueil de données d'efficacité et de tolérance. Son pouvoir de sanction est renforcé et assorti d'amendes financières.

L'Agence est non seulement une agence d'évaluation et d'expertise mais aussi une agence investie d'une large délégation de puissance publique qui prend, au nom de l'État, plus de 80 000 décisions par an (notamment dans le cadre des procédures d'autorisation et d'interdiction qu'elle met en œuvre). Elle exerce des missions propres d'évaluation avant et après la mise sur le marché, de contrôle des produits en laboratoires, d'inspection sur les sites de production, de distribution en gros ou d'essais cliniques. En outre, elle élabore et diffuse auprès des professionnels de santé et des patients des informations destinées à favoriser le bon usage des produits de santé. Elle s'inscrit également dans les démarches de santé publique et contribue aux différents plans et programmes de santé engagés par les pouvoirs publics.

L'effectif de l'ANSM est actuellement de l'ordre de 1000 agents répartis sur trois sites : Saint-Denis, siège administratif et de l'hébergement du cœur des infrastructures informatiques de l'Agence, Lyon et Vendargues (dans l'agglomération de Montpellier).

Tous renseignements utiles au titulaire, relatifs à l'activité de l'Agence, ses compétences et son organisation peuvent être trouvés sur son site Internet à l'adresse suivante : <https://ansm.sante.fr>.

### 1.2. Objet du marché

---

L'ANSM souhaite disposer :

- d'une infrastructure évolutive et au plus près de « l'état de l'art »,
- d'une richesse de niveaux de services (différentes classes de stockages, différentes classes de serveurs virtuels, ...) payables à l'usage.

Les prestations attendues du Titulaire sont :

- le support utilisateurs notamment des chefs de projet informatiques,
- le support aux équipes techniques de l'ANSM pour les phases d'interconnexion avec son réseau,
- la mise à disposition de capacités informatiques « à la demande » en infrastructure virtuelle ou en serveurs physiques hébergées dans des centres de données (datacenter) fournissant le niveau de sécurité, la garantie et la disponibilité d'une puissance électrique suffisante (datacenter a minima conformes aux normes Tier III+ ou équivalent, voire Tier IV), et d'un impact environnemental contenu,
- La capacité à héberger des données de santé,
- La capacité à fournir des infrastructures permettant la mise en place d'un plan de reprise d'activité (PRA) pour certaines applications,
- La mise à disposition de services d'infogérance et prestations associées,
- la mise à disposition et la gestion d'un service de sauvegarde et restauration,
- l'assistance technique,
- la gouvernance des prestations,
- la gestion de la réversibilité entrante et sortante.

Un des enjeux majeurs est la capacité à héberger des applications gérants des données de santé. Le titulaire doit donc obligatoirement être certifié HDS (hébergeur de données de santé) ou au moins être

en partenariat avec un hébergeur certifié HDS. Il doit aussi être en capacité de fournir des infrastructures permettant la mise en place d'un plan de reprise d'activité sur un site secondaire.

En outre, le titulaire du marché doit contribuer aux enjeux du développement durable, et donc présenter dans son offre et mettre en œuvre une démarche RSE (Responsabilité sociale et environnementale - <https://www.ecologie.gouv.fr/responsabilite-societale-des-entreprises> ou <https://www.economie.gouv.fr/entreprises/responsabilite-societale-entreprises-rse>).

Enfin, il est attendu du Titulaire qu'il soit en capacité de fournir sur demande un hébergement de type Cloud souverain pour certaines données qui seraient jugées particulièrement sensibles, y compris par le recours à un partenaire (sous-traitant qualifié SecNumCloud).

Le présent document décrit les services attendus.

Le Titulaire s'engage à fournir une offre et un service conformes aux spécifications contenues dans l'ensemble des pièces contractuelles du présent marché.

### 1.3. Définitions

---

Dans le présent CCTP ainsi que ses annexes, sont désignés sous le terme de :

- ANSM : Agence Nationale de Sécurité du Médicament et des Produits de Santé ;
- Le terme « Pouvoir Adjudicateur » désigne l'ANSM ;
- Titulaire – l'opérateur économique (y compris le cas échéant le groupement d'opérateurs économiques) qui conclut le présent marché avec le Pouvoir Adjudicateur ;
- PAQ – Plan d'Assurance Qualité : ce plan, fourni par le Titulaire, doit décrire la gouvernance relative à la gestion de la qualité et au pilotage des prestations, le suivi de la qualité ;
- PAS – Plan d'Assurance Sécurité : ce plan, fourni par le Titulaire, doit décrire la gouvernance relative à la gestion de la sécurité, le suivi des risques et leurs modalités de prise en compte ;
- BPU – Bordereau des Prix Unitaires (annexe financière de l'acte d'engagement) du présent marché public ;
- UO – Unité(s) d'œuvre ;
- VM – Machine Virtuelle ;
- HDS – Hébergeur (ou hébergement selon les cas) de Données de Santé ;
- Infrastructure virtuelle – un ensemble d'infrastructures fournies comme des services (IaaS/PaaS), supportées par des ressources matérielles, et gérée par le Titulaire (intégrant les activités de supervision, maintenance, exploitation ...) ;
- Risque de perte de site – tout événement lié au Datacenter (incendie, inondation, qui rendrait partiellement ou totalement indisponibles les infrastructures informatiques hébergées du Pouvoir Adjudicateur) ;
- Capacités – terme générique pour décrire quantitativement tous types de ressources nécessaires au bon fonctionnement du SI de l'ANSM (CPU, RAM, VM, Stockage, Bande Passante, ...). Les « capacités » sont associées à des « dispositifs techniques » (serveurs, baies de stockage, ...) ;
- Outil(s) ITSM : outil(s) de gestion des services informatiques du Titulaire et accessible au Pouvoir Adjudicateur ;
- GTI : Garantie de Temps d'Intervention. Délai maximal entre l'ouverture d'un ticket d'incident (ou la détection automatique par les outils du Titulaire) et le début effectif des actions techniques de résolution réalisées par un technicien qualifié du Titulaire (niveau 2 ou niveau 3). Ce délai inclut l'organisation de l'intervention, la mobilisation des ressources nécessaires et l'engagement effectif sur la résolution. Le point de départ du délai de GTI est la date et l'heure d'horodatage du ticket d'incident dans l'Outil ITSM du Titulaire. La GTI varie selon le niveau de criticité des incidents conformément à la convention de service (annexe 2 du CCTP).
- GTR : Garantie de Temps de Rétablissement. Délai maximal entre l'ouverture d'un ticket d'incident (ou la détection automatique par les outils du Titulaire) et le rétablissement complet du service affecté, permettant son fonctionnement nominal conformément aux performances attendues. Le rétablissement implique la correction de la cause de l'incident, la remise en fonctionnement stable du service, et la validation technique par le Titulaire. Le point de départ du délai de GTR est la date et l'heure d'horodatage du ticket d'incident dans l'Outil ITSM du Titulaire. Le point de fin est l'horodatage du retour au fonctionnement nominal validé par le

Titulaire dans l'outil ITSM. La GTR varie selon le niveau de criticité des incidents conformément à la convention de service (annexe 2 du CCTP).

- PRA : Plan de reprise d'activité. Dans le cadre de ce CCTP, le service de PRA désigne la mise en place d'une architecture multi-sites résiliente pour les services désignés comme critiques, avec réplication des données et des applications vers un site secondaire géographique distinct et redondance des composants critiques.

#### 1.4. Objectifs

---

En confiant tout ou partie de la gestion de l'hébergement au Titulaire, le Pouvoir Adjudicateur attend :

- Un maintien à l'état de l'art des infrastructures informatiques objets du présent marché en termes de sécurité, disponibilité et administration,
- un engagement de résultat en termes de fiabilité et de disponibilité,
- une pleine prise en compte des contraintes et directives propres à l'hébergement des données,
- une grande flexibilité pour accompagner le développement du Pouvoir Adjudicateur et des services proposés,
- la capacité à satisfaire aux niveaux de criticité des applicatifs stratégiques et dont l'environnement d'utilisation nécessite une disponibilité 24h/24 et 7j/7.

## 2. PRÉSENTATION DU CONTEXTE

---

### *Présentation du périmètre SI inclus dans le marché*

---

Le périmètre hébergé par le titulaire en place au 1<sup>er</sup> décembre 2025 est décrit dans l'annexe 1 du CCTP « Fiche architecture technique ».

Le présent marché doit permettre d'assurer la reprise, l'hébergement et les services associés à ce périmètre, ainsi qu'aux applications qui seront mises en place postérieurement (que ce soit suite à leur installation ou commencement d'utilisation par l'ANSM ou d'une migration de données que le Titulaire devra réaliser).

Le périmètre des applications hébergées dans le cadre de ce marché pourra dans tous les cas varier à tout moment, à la hausse comme à la baisse, en fonction des besoins de l'ANSM. Ainsi, le Titulaire pourra également être amené à réaliser la réversibilité sortante des données d'une application en cours de marché vers l'infrastructure de l'ANSM ou d'un tiers en cas de passage en SaaS de ladite application.

Les applications de l'ANSM sont hébergées dans deux zones distinctes :

- Une zone « Bunker », accessible uniquement depuis l'ANSM via un VPN dédié,
- Une zone « internet » pour exposer des services sur internet.

## 3. PHASES DU MARCHÉ

---

### 3.1. Présentation générale des phases

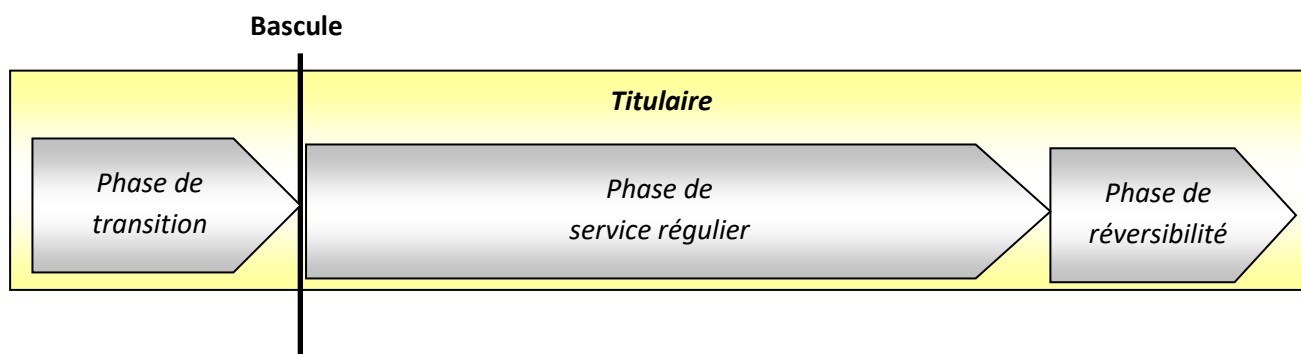
---

La prestation est constituée de trois (3) phases :

- Phase de transition ou réversibilité entrante (est déclenchée au début du marché par bon de commande qui fixe les délais et ses modalités d'exécution) :
  - Caractéristique : cette phase de transition a pour objectif de migrer les applications de l'ANSM hébergées par le titulaire sortant du marché : il s'agit de la période pendant laquelle le service souscrit est mis en place.
  - Activités principales :
    - Prise en charge : mise en place de l'ensemble des moyens (organisation, formation, outil, technologie, processus, procédures, documentation, ...) nécessaires à la réalisation du service et prise de connaissance de l'existant ;
    - Élaboration et mise en œuvre du plan de migration des infrastructures de l'hébergeur de l'ANSM vers le Titulaire.

- Fin : validation par le Pouvoir Adjudicateur de la mise en services des applications de l'ANSM (suite à la Vérification d'aptitude - VA).
- Phase de service régulier (phase récurrente) :
  - Début : validation par le Pouvoir Adjudicateur du caractère opérationnel du service et du respect des engagements de niveaux de service ;
  - Caractéristique : période pendant laquelle le service est effectif, les engagements de niveaux de service contractuels et les pénalités applicables ;
  - Activité principale : réalisation du plan d'exécution de service en vigueur ;
  - Fin : le Titulaire du marché assure un service régulier jusqu'à la fin du marché y compris lorsque la réversibilité est engagée à la demande du Pouvoir Adjudicateur.
- Phase de réversibilité sortante (déclenchée par bon de commande qui fixe les délais et ses modalités d'exécution) :
  - Début : à la date d'échéance du marché (sauf en cas de réversibilité anticipée) ;
  - Nature : période de transfert de connaissances, et de mutation des services souscrits vers un nouveau Titulaire ou le Pouvoir Adjudicateur, le cas échéant ;
  - Activité principale : fourniture de la totalité de la documentation et des éléments réversibles, et transfert de compétences, mutation des services, transfert des données vers le nouveau prestataire ou le Pouvoir Adjudicateur, le cas échéant.

L'ordonnancement des phases est schématisé ci-dessous.



Le planning détaillé des différentes phases peut être ajusté à la notification du marché et peut continuer d'évoluer au cours de la prestation sous réserve de validation formelle des deux parties.

A chaque phase, le Pouvoir Adjudicateur se réserve le droit de différer l'engagement (et la facturation) de la phase suivante s'il considère que les travaux et services fournis ne correspondent pas aux attentes et nuisent à la qualité de service des phases suivantes.

Il est rappelé explicitement que le démarrage d'une phase ne vaut pas procès-verbal d'acceptation de la phase précédente.

### 3.2. Détail de la phase transition (réversibilité entrante)

#### 3.2.1. Périmètre

L'objectif de la phase de transition est le transfert et la mise en service de l'ensemble des applications et sites hébergés sur les plateformes de l'hébergeur actuel (et listés à l'annexe 1 au présent CCTP) en état de fonctionnement.

La description des infrastructures des applications actuellement hébergées et à prendre en charge sont décrites dans l'annexe suivante :

- Annexe 1 - Hébergement - Fiche architecture technique.

### 3.2.2. Prestations attendues

N.B. : les UO en face de chaque ensemble de prestations, font références aux unités d'œuvre du BPU.

Les étapes et livrables a minima attendus de cette phase sont les suivants :

- **Prise en charge du marché UO\_Transition\_1.1 : Audit de l'architecture technique** comprenant notamment :
  - Réunion de lancement (présentation des équipes, présentation de la démarche de mise en œuvre) ;
  - Réalisation de la matrice de responsabilité (RACI) conjointement avec le Pouvoir Adjudicateur ;
  - Validation de la gouvernance de transition (les dispositifs de pilotage, les indicateurs de suivi, ...) ;
  - Analyse des risques ;
  - Identification des prérequis propres au Titulaire et au Pouvoir Adjudicateur ;
  - Planification détaillée des chantiers / ateliers :
    - ✓ Appropriation du contexte,
    - ✓ Processus et Outils ITSM,
    - ✓ Outils techniques (supervision, stockage, sauvegarde, ...),
    - ✓ Telecom / Infrastructures / Sécurité qui permettent d'élaborer notamment le PAS,
    - ✓ Gouvernance (indicateurs de qualité de service, facturation) qui permettent notamment d'élaborer le PAQ ;
  - Les livrables attendus sont les suivants :
    - ✓ Plan de transition (Démarche, dispositifs de pilotage, indicateurs de suivi, planification des chantiers et de ateliers, ...),
    - ✓ Toutes les annexes adaptatives dans une version de travail qui permet d'initier les travaux en atelier,
    - ✓ Le PAS,
    - ✓ Le PAQ.
- **Prise en charge du marché UO\_Transition\_1.2 : Définition du dossier de migration** avec :
  - Récupération par le Titulaire du référentiel documentaire à jour du Pouvoir Adjudicateur,
  - Revue des types d'accès aux plateformes autorisés par le titulaire sortant,
  - Prise de connaissance détaillée de la politique de sécurité de l'ANSM et mise en application pratique,
  - Définition et conception du plan de migration pour les environnements demandés : support utilisateurs, socle hébergement (cf modules A1 et A3.x décrits ci-dessous),
  - Elaboration du plan de recette du service permettant au Titulaire de valider que le service sera rendu au niveau attendu,
  - Les livrables attendus sont les suivants :
    - ✓ Plan de migration des services,
    - ✓ Plan de recette des services : technique, documentaire, reporting...
- **Mise en œuvre UO\_Transition\_2.1 et 2.2 : Déploiement des infrastructures et environnements et migrations des applications** avec :
  - Réalisation de la mise en œuvre du Plan de Migration des infrastructures,
  - Paramétrage des outils techniques et de l'outil ITSM du Titulaire (par exemple : création des groupes support, indicateurs contractuels, indicateurs opérationnels, facturation),
  - Construction des indicateurs opérationnels d'exploitation (contrôles matinaux, rapports de supervision, ...),
  - Réalisation de la recette pour vérification d'aptitude au bon fonctionnement (VA) :
    - ✓ Le Titulaire déclenche la recette de Vérification d'Aptitude (« VA ») de la prestation à la fin de l'installation de l'ensemble des applications ;
    - ✓ Le Titulaire assure une assistance pendant toute la phase de recette. Si lors de ces tests, des anomalies sont constatées, elles sont immédiatement prises en compte et corrigées par le Titulaire.



- ✓ A l'issue de cette période de tests, le Pouvoir Adjudicateur prend une décision concernant la VA conformément aux stipulations du Cahier des Clauses Administratives Particulières (CCAP) relatives à la vérification des prestations.
- ✓ La VA ne peut être effective que lorsque l'ensemble des applications installées sur les plateformes du Pouvoir Adjudicateur est opérationnel.

La recette prononcée par les parties, la réalisation du service est effective et opérationnelle.

Les livrables minima attendus pour permettre la vérification d'aptitude par l'ANSM sont les suivants :

- Mise à jour des annexes contractuelles (PAQ, PAS, convention de services....),
- Cahier de recette de la VA.

Tous les livrables sont validés par écrit par le Pouvoir Adjudicateur, cette validation étant officialisée par la signature d'un procès-verbal d'acceptation.

A l'issue de la vérification d'aptitude et en cas de décision positive du Pouvoir Adjudicateur débute la phase de service régulier.

### 3.2.3. Modèle Financier

---

La rémunération des prestations demandées se fait selon le modèle d'UO du BPU.

La phase de transition est ainsi rémunérée par :

- Un forfait de prise en charge du marché indépendant du nombre et de la complexité des applications (UO\_Transition\_1.1),
- Un forfait global pour la définition du dossier de migration pour chacune des applications (UO\_Transition\_1.2),
- Un forfait pour la mise en œuvre concernant le déploiement des infrastructures et environnements ainsi que la migration des sites et applications (UO\_Transition\_2.1 et UO\_Transition\_2.2),
- Les prix d'initialisation des services des unités d'œuvre des différents modules à activer pour la mise en œuvre de la connexion internet (soit les UO de mise en service du module A2) et de l'ensemble des plateformes (UO de mise en service des modules A3.x),
- Les prix d'initialisation de l'infogérance et des services associés (UO de mise en service du module A4).

### 3.3. Détail de la phase de service régulier

---

Les prestations attendues en service régulier sont décrites au chapitre 4 – Prestations attendues d'hébergement.

Le Titulaire peut également en cours de marché avoir à réaliser une réversibilité entrante partielle et une recette de Vérification d'Aptitude (« VA ») dans le cas de bons de commande associés à la mise en place de services ou d'applications à la fin de l'installation desdits services ou applications. Ces prestations font alors l'objet de vérifications qualitatives conformément aux stipulations du Cahier des Clauses Administratives Particulières (CCAP). Ces prestations seront le cas échéant mises en œuvre par la commande de diverses UO prévues au BPU du présent marché.

### 3.4. Détail de la phase de réversibilité (sortante)

---

#### 3.4.1. Périmètre

---

Dans le cadre du présent marché, le Titulaire s'engage à assurer la réversibilité du service à la fin du marché (y compris en cas de non-renouvellement ou résiliation anticipée) afin de permettre au Pouvoir Adjudicateur de reprendre ou de faire reprendre par un tiers la fourniture du service et ce, dans les meilleures conditions et sans discontinuité du service.



La réversibilité est déclenchée par un bon de commande qui précise sa durée, sa mise en œuvre et ses modalités d'exécution.

N.B. : les unités d'œuvres (UO) en face de chaque ensemble de prestations, font référence aux unités d'œuvre du BPU décrites ci-après.

### 3.4.2. Prestations attendues

---

#### a. UO\_A7\_1 – Rédaction du plan de réversibilité

---

Le plan de réversibilité est un document qui doit détailler le processus de transfert de la maintenance et de l'exploitation de la solution à un autre prestataire ou au Pouvoir Adjudicateur, conformément aux exigences légales (RGPD, HDS) et aux bonnes pratiques (ISO 27001, ANSSI).

Le plan de réversibilité est mis à disposition du Pouvoir Adjudicateur pour revue et validation sous trente (30) jours après commande de l'UO.

En outre, la phase de réversibilité ne doit pas altérer la qualité, les termes et les conditions de service régulier fournis durant l'exécution du marché.

Le plan de réversibilité doit inclure les éléments suivants :

- Les différents acteurs du processus de transfert avec leur rôle et responsabilité,
- Le scénario de réversibilité avec toutes les étapes,
- La gestion des biens (inventaire, configuration...),
- La liste des contrats de support et documents à transférer,
- L'analyse des dépendances : cartographie des services, applications, données et infrastructures à reverser,
- Les procédures détaillées :
  - Étapes techniques (export des données, migration, tests),
  - Rôles et responsabilités (Titulaire, Pouvoir Adjudicateur, sous-traitants).
  - Calendrier prévisionnel et jalons.

Les livrables sont :

- Le plan de réversibilité,
- Des checklists opérationnelles pour chaque type de service (serveurs, réseau, applications).

Exigences :

- Conformité aux exigences HDS (pour les applications concernées) et au RGPD (portabilité des données),
- Validation par le Pouvoir Adjudicateur avant mise en œuvre.

#### b. UO\_A7\_2 – Réversibilité Connexion Internet et services réseau

---

Le Titulaire assurera la restitution des configurations réseau et la continuité des services de connectivité. Il devra apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des infrastructures et la reprise de leur exploitation par le Pouvoir Adjudicateur, ou par un tiers.

Périmètre :

- Connexion Internet : Restitution des adresses IP, règles de pare-feu, DNS, et VPN ;
- Services réseau : Réversibilité des load balancers, VLAN, et routes statiques ;
- Transfert à l'équipe du futur titulaire des informations sur le contexte technique.

Livrables :

- Export des configurations (fichiers standardisés : JSON, YAML, ou formats éditeurs) ;
- Documentation technique : Schémas d'architecture, dépendances, et procédures de migration.

Exigences :

- Délai maximal : quinze (15) jours ouvrés après la commande pour la restitution complète ;
- Format des données : Compatible avec les standards du marché (ex : Cisco, Juniper, AWS/Azure) ;
- Support : Assistance technique pendant trente (30) jours après la réversibilité.

c. UO\_A7\_3 – Réversibilité des serveurs (Simple : 50 machines)

---

Objectif de migration des serveurs et leurs données vers un nouvel environnement (cloud ou on-premise) sans interruption de service pour cinquante (50) machines. Le forfait inclut la coordination avec les équipes du Pouvoir Adjudicateur et / ou le titulaire du nouveau marché.

Le Titulaire apportera l'assistance nécessaire durant la période de migration pour faciliter le transfert des infrastructures et la reprise de leur exploitation par le Pouvoir Adjudicateur, ou par un tiers.

Il devra en outre transférer le cas échéant à l'équipe du futur titulaire des informations sur le contexte fonctionnel et technique de l'ensemble applicatif, ainsi que sur les aspects de suivi du projet.

Périmètre :

- Serveurs concernés : Machines virtuelles ou physiques (OS Linux/Windows),
- Données : Export des volumes de stockage, bases de données, et configurations,
- Applications : Conteneurs ou applications monolithiques (sans dépendances complexes).

Livrables :

- Images disques (format OVF, VMDK, ou QCOW2) ou snapshots cohérents,
- Scripts d'automatisation pour le redéploiement (Ansible, Terraform, ou équivalent),
- Rapport de migration : Inventaire, statuts, et logs des opérations,
- Fourniture de la documentation pour toutes les applications.

Exigences :

- Disponibilité : 99 % pendant la migration,
- Intégrité des données : Vérification par checksum (SHA-256).

d. UO\_A7\_4 – Réversibilité par serveur supplémentaire

---

Migrer un serveur et ses données vers un nouvel environnement (cloud ou on-premise) sans interruption de service. Le forfait inclut la coordination avec les équipes de l'ANSM et / ou le titulaire du nouveau marché.

Le Titulaire apportera l'assistance nécessaire durant la période de migration pour faciliter le transfert des infrastructures et la reprise de leur exploitation par le Pouvoir Adjudicateur, ou par un tiers.

Il devra en outre transférer le cas échéant à l'équipe du futur titulaire des informations sur le contexte fonctionnel et technique de l'ensemble applicatif ainsi que sur les aspects de suivi du projet.

Périmètre :

- Serveurs concernés : Machines virtuelles ou physiques (OS Linux/Windows),
- Données : Export des volumes de stockage, bases de données, et configurations,
- Applications : Conteneurs ou applications monolithiques (sans dépendances complexes).

Livrables :

- Images disques (format OVF, VMDK, ou QCOW2) ou snapshots cohérents,
- Scripts d'automatisation pour le redéploiement (Ansible, Terraform, ou équivalent),
- Rapport de migration : Inventaire, statuts, et logs des opérations,

- Fourniture de la documentation pour toutes les applications.

Exigences :

- Disponibilité : 99 % pendant la migration,
- Intégrité des données : Vérification par checksum (SHA-256).

### 3.4.3.Modèle Financier

---

La rémunération des prestations demandées se fait selon le modèle d'UO proposé dans le BPU.

Cette rémunération est constituée de :

- Un forfait global pour la rédaction du plan de réversibilité et le pilotage de cette phase (UO\_A7\_1) ;
- Un forfait pour la réversibilité de la connexion Internet et des services réseau (UO\_A7\_2) ;
- Un forfait de base pour la réversibilité de 50 serveurs applicatifs (UO\_A7\_3) ;
- Autant d'UO\_A7\_4 que de serveurs restants (nombre total de serveurs – 50).

### 3.4.4.Réversibilité sortante partielle

---

Nonobstant les stipulations précédentes, le Titulaire peut également en cours de marché avoir à réaliser une réversibilité sortante partielle d'une application ou d'un service en cours de marché vers l'infrastructure de l'ANSM ou d'un tiers en cas d'arrêt du service, ou encore en cas de réinternalisation de l'hébergement et/ou de passage en SaaS de ladite application. Ces prestations seront le cas échéant mises en œuvre par la commande de diverses UO prévues au BPU du présent marché.

## 4.PRESTATIONS ATTENDUES D'HÉBERGEMENT

---

### 4.1. Introduction

---

Les prestations attendues sont découpées en modules. Chaque module correspond à une ou plusieurs fonctions identifiées comme pouvant être associées à une équipe, à un profil d'intervenants ou à un dispositif de tarification.

Ce découpage en modules ne préjuge pas de l'organisation des moyens du Titulaire. Il est attendu du Titulaire qu'il organise ses équipes et moyens pour atteindre la meilleure rationalisation des coûts et la meilleure efficacité du service possible.

Les modules ainsi définis sont les suivants :

- Module A1 - Support aux utilisateurs
- Module A2 - Fourniture d'une connexion Internet
- Module A3.1 - Fourniture de capacités de type Infrastructure virtuelle
- Module A3.2 - Fourniture de serveurs physiques
- Module A4 - Service d'infogérance et prestations de service associé
- Module A5 - Assistance technique et prestations complémentaires
- Module A6 – Pilotage et accompagnement

### 4.2. Evolution vers des hébergements Cloud souverain / SecNumCloud

---

Le présent paragraphe a pour objet de définir les exigences relatives à la capacité du Titulaire à évoluer vers un hébergement souverain, conforme au référentiel SecNumCloud publié par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), ou vers un dispositif équivalent reconnu par ladite agence.

Le Pouvoir Adjudicateur n'exige pas, à la date de notification du présent marché, que le Titulaire dispose d'une qualification SecNumCloud effective.

En revanche, le Titulaire doit justifier, dès la présentation de son offre, de l'engagement formel de la démarche de qualification auprès de l'ANSSI, dite étape « J0 ANSSI », matérialisée par :

- le dépôt d'un dossier de candidature complet auprès de l'ANSSI, ou
- une attestation délivrée par un prestataire d'audit qualifié confirmant le lancement de la procédure d'évaluation, ou
- tout document officiel émanant de l'ANSSI confirmant l'enregistrement de la démarche SecNumCloud.

Cette exigence vise à s'assurer que le Titulaire est activement engagé dans un processus de qualification, garantissant à terme la conformité de ses environnements souverains au référentiel SecNumCloud.

Le Titulaire pourra également recourir aux services d'un sous-traitant hébergeur qualifié SecNumCloud, mais devra dans ce cas justifier, dès la présentation de son offre et à tout moment au cours de l'exécution du marché (sur simple demande de l'ANSM), de la qualification SecNumCloud de son sous-traitant et du partenariat durable avec ce sous-traitant. Le partenariat devra être maintenu durant toute la durée du marché, de sorte que le Titulaire pourra à tout moment répondre à une demande du Pouvoir Adjudicateur relative à un hébergement SecNumCloud.

Aucune prestation effective d'hébergement en environnement SecNumCloud n'est exigée au démarrage du marché.

Le Pouvoir Adjudicateur souhaite uniquement s'assurer que le Titulaire est en mesure, à l'issue du processus de qualification engagé ou à tout moment en cas de recours à un sous-traitant, de proposer une offre d'hébergement souveraine conforme au référentiel ANSSI, utilisable dans le cadre de marchés subséquents.

Si, au cours de l'exécution de l'accord-cadre, un besoin d'hébergement souverain devait émerger (par exemple pour des applications traitant des données sensibles, stratégiques ou de santé), le Pouvoir Adjudicateur pourra lancer, conformément aux stipulations du CCAP, un marché subséquent afin d'activer les prestations d'hébergement SecNumCloud.

Le Titulaire lorsque la qualification sera obtenue ou son sous-traitant devra garantir :

- la localisation intégrale des données et traitements sur le territoire français,
- la souveraineté juridique complète, excluant toute soumission à des législations extraterritoriales non européennes,
- la traçabilité et l'auditabilité des opérations conformément au référentiel ANSSI,
- la réversibilité totale des données et configurations vers tout autre environnement qualifié.

La solution du Titulaire peut reposer sur une architecture multi-cloud combinant différents régimes d'hébergement (Standard, HDS, SecNumCloud).

Le Titulaire devra garantir que les workloads critiques pourront, le moment venu, être hébergés exclusivement dans un environnement souverain, qualifié et audité, sans dépendance technologique ou contractuelle à des prestataires non conformes au référentiel SecNumCloud.

Dans tous les cas, le Titulaire sera responsable de l'exécution des prestations par son sous-traitant.

Toute perte de qualification SecNumCloud du Titulaire ou de son sous-traitant, ou rupture du partenariat avec le sous-traitant qualifié SecNumCloud, devra être immédiatement signalée par écrit au Pouvoir Adjudicateur (et dans un délai maximum de deux jours ouvrés). Le Titulaire devra alors proposer une solution alternative, soit immédiatement en cas de besoin d'un tel hébergement par le Pouvoir Adjudicateur, soit dans un délai convenu entre les parties en l'absence d'un tel besoin.

### **4.3. Dispositions communes à l'ensemble des modules**

---

#### **4.3.1. Outillage de service**

---

Dans le cadre de la prestation, le Titulaire doit fournir un outil de gestion permettant notamment :

- la déclaration directe d'incidents par le Pouvoir Adjudicateur et l'envoi par courriel d'accusés de réception correspondants ;

- la déclaration directe de demandes de services définis dans le paragraphe 4.9.2 ;
- le suivi en temps réel du traitement des incidents et demandes par le Pouvoir Adjudicateur ;
- la production des indicateurs de niveaux de services demandés et le reporting de suivi opérationnel ;
- l'administration des composants mis à disposition dans le cadre des modules A3.1 et A3.2 – fourniture des capacités : création / modification de VM, création / modification d'espace de stockage, récupération de sauvegarde, restauration de données, ....

Les dispositifs de communication (envoi – réception de courriels, numéro de téléphone) doivent être également fournis.

Le Titulaire mettra en place une supervision en temps réel des infrastructures et services hébergés, incluant :

- Un système d'alertes proactives (via email) pour les événements critiques (ex : indisponibilité, saturation des ressources, tentatives d'intrusion), avec des seuils personnalisables et une escalade automatique vers les équipes techniques ;
- Un dashboard partagé (accessible 24 heures sur 24 et 7 jours sur 7 via une interface sécurisée) affichant les métriques clés : disponibilité des services, performances (latence, débit), consommation des ressources (CPU, RAM, stockage), et statut des sauvegardes.

Le Titulaire doit également disposer d'un outil de suivi financier et d'optimisation des coûts pour la prestation, ainsi qu'un outil de gestion documentaire.

L'ensemble de ces outils doivent être accessibles par le biais d'une interface web.

La mise à disposition des outillages de service ne fait pas l'objet d'un surcoût dédié. Le coût lié à la mise à disposition est réputé compris dans les unités d'œuvres des différents modules.

#### 4.3.2. Interopérabilité et réversibilité

---

Pour garantir une ouverture et faciliter la réversibilité, tous les services, infrastructures et données devront être conçus et exploités en s'appuyant autant que possible sur des standards ouverts et interopérables. Cela inclut :

- APIs standardisées (REST, OpenAPI/Swagger) pour les échanges de données et l'intégration avec les systèmes tiers,
- Formats de sauvegarde et d'export non propriétaires (ex : OVF/OVA pour les machines virtuelles, SQL pour les bases de données, JSON/CSV pour les données structurées),
- Infrastructure as Code (IaC) avec des outils comme Terraform (modules publics) ou Ansible (playbooks documentés) pour la gestion et le déploiement des ressources,
- Conteneurs (Docker, OCI) et orchestration (Kubernetes CNCF) pour les applications, avec des images compatibles avec tout environnement conforme aux standards du marché. Ces exigences visent à éliminer tout risque de dépendance technique et à permettre une migration fluide vers un autre hébergeur ou une infrastructure interne à l'ANSM, sans perte de fonctionnalités ni coûts cachés. Le Titulaire devra fournir, à tout moment et sans supplément, la documentation complète et les artefacts nécessaires (codes, configurations, schémas) pour assurer une réversibilité immédiate et sans rupture de service.

#### 4.3.3. Contraintes de service

---

Les activités des modules pour lesquelles un niveau de service est attendu de la part du Titulaire sont listées dans la convention de services.

L'ensemble des activités listées dans les différents modules a pour vocation d'illustrer l'attendu avec des activités usuelles de ce type de prestation, mais ne se veut pas exhaustif. Il est entendu que le Titulaire réalise toutes les actions et activités nécessaires au respect des niveaux de service tels qu'ils seront commandés par le Pouvoir Adjudicateur.

Par ailleurs, les prestations fournies au titre des différents modules doivent être conformes à la politique de sécurité des systèmes d'information du Pouvoir Adjudicateur (partiellement explicitée dans les

documents du marché et que le Pouvoir Adjudicateur pourra détailler et/ou préciser au Titulaire sur simple demande) et à ses déclinaisons thématiques ainsi que la réglementation en vigueur applicable au Pouvoir Adjudicateur.

#### 4.3.4.Plages de services

---

Les services des différents modules sont assurés et accessibles 24 heures sur 24 et 7 jours sur 7. La plage de service permanente est du lundi au vendredi de 9h00 à 18h00, hors jours fériés légaux. Au-delà de cette plage de service, le Titulaire organise les astreintes selon les classes de services attendues.

#### 4.3.5.Documentation et Capitalisation

---

Le Titulaire conçoit et maintient une documentation opérationnelle (PAQ, plan de réversibilité, Dossier d'architecture technique...), qu'il mettra à la disposition du Pouvoir Adjudicateur lors de la phase de transition.

Le Titulaire est responsable de la mise à jour du référentiel documentaire constitué pour le bon fonctionnement de chacun des modules sur lequel il opère.

#### 4.3.6.Règles de sécurité

---

##### a. Préambule

---

La protection de la part hébergée du système d'information (SI) du Pouvoir Adjudicateur et des informations qu'elle contient demande un engagement du Titulaire quant au respect des règles de sécurité des systèmes d'information, que ce soit en termes de confidentialité, d'intégrité ou de traçabilité, tout autant que de disponibilité.

Pour réaliser leur mission, les équipes du Titulaire doivent avoir de bonnes connaissances en sécurité des systèmes d'information et être sensibilisées au respect de la politique et des règles de sécurité applicables au SI du Pouvoir Adjudicateur. Le Titulaire assure la sensibilisation, et si nécessaire la formation, de ses équipes dans ce sens. Un suivi est communiqué annuellement au Pouvoir Adjudicateur.

##### b. Règles générales

---

Le Titulaire doit mettre en œuvre ou appliquer toutes les mesures nécessaires à la protection permanente des infrastructures, plateformes et données du Pouvoir Adjudicateur, en conformité avec les exigences suivantes, applicables sur l'ensemble du périmètre des prestations :

- Norme ISO/IEC 27001:2022 (et son annexe A actualisée) pour le management de la sécurité de l'information (SMSI), incluant les contrôles complémentaires de la norme ISO/IEC 27002:2022 (bonnes pratiques de sécurité) ;
- Référentiel Général de Sécurité (RGS) v2.0 (<https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents> ), notamment pour les exigences de chiffrement, authentification forte et journalisation ;
- Guide de l'ANSSI sur la sécurisation des prestations d'hébergement externalisé (version 2023 : <https://cyber.gouv.fr/publications/guide-dhygiene-informatique>) ;
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la Protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (autrement appelé « RGPD ») ([UE 2016/679](#)) ;
- NIS 2 ([Directive UE 2022/2555](#)), applicable depuis octobre 2024, pour les opérateurs de services essentiels (incluant les hébergeurs cloud), avec des obligations renforcées en matière de détection des incidents, notification (délai ≤ 24h pour les incidents majeurs) et résilience.

Le titulaire devra documenter et maintenir à jour :

- Une cartographie des risques (alignée sur la norme ISO 27005:2022),
- Un plan de traitement des risques incluant les mesures techniques et organisationnelles (ex : chiffrement des données au repos et en transit, segmentation réseau, sauvegardes immutables),



- Les preuves de conformité (audits, certifications, rapports de tests d'intrusion), transmises annuellement au Pouvoir Adjudicateur.

Les solutions d'hébergement des sites et des applications du Pouvoir Adjudicateur doivent être en accord avec le droit français et avec les éventuelles recommandations de la Commission nationale de l'informatique et des libertés (CNIL).

**De plus, dans le cadre des applications métiers ou des répliques de données métier, le Pouvoir Adjudicateur a besoin d'héberger des données de santé qui tombent sous le coup de la réglementation en vigueur (Hébergement Agréé Données de Santé - HDS).**

Le Titulaire reconnaît avoir pris connaissance des obligations légales et réglementaires applicables à l'hébergement de données de santé à caractère personnel. Il s'engage à disposer, pendant toute la durée d'exécution du marché, d'une certification HDS (Hébergement des Données de Santé) en cours de validité pour l'ensemble des activités et modules concernés conformément au BPU, délivrée par un organisme accrédité, conformément aux dispositions de l'article L.1111-8 du Code de la santé publique et du décret n° 2018-137 du 26 février 2018 relatif à l'hébergement des données de santé à caractère personnel dans sa version consolidée applicable au lancement de la consultation et à tout moment au cours de l'exécution du marché public. À défaut de disposer de cette certification, le Titulaire devra justifier d'un partenariat avec un hébergeur certifié HDS, garantissant le respect des exigences légales en matière de sécurité, de confidentialité et de traçabilité des données. La perte de la certification HDS en cours d'exécution du marché, ou la rupture du partenariat avec un hébergeur certifié HDS, constituera un manquement grave et pourra entraîner la résiliation du marché pour faute du Titulaire conformément aux stipulations du CCAP, sauf si le Titulaire propose, dans un délai imparti par l'ANSM, une solution alternative permettant d'assurer la continuité du service dans des conditions conformes aux exigences légales et contractuelles.

Le Titulaire est tenu de communiquer au Pouvoir Adjudicateur toutes modifications (perte, renouvellement etc...) qui aurait un impact sur l'agrément initialement fourni.

Toutes les UO portant le suffixe « \_HDS » dans le présent document intègrent par défaut les exigences d'un Plan de Reprise d'Activité (PRA) complet (réplication multisite des données et infrastructures vers un site secondaire géographiquement distinct, objectifs de reprise avant 2h, ...).

Le Titulaire s'engage également :

- à effectuer une veille régulière pour suivre les évolutions réglementaires et les mettre en œuvre,
- à accepter des audits sécurité et des tests d'intrusion réalisés à la demande du Pouvoir Adjudicateur. A réception des résultats d'audit et des états de vulnérabilité communiqués par le Pouvoir Adjudicateur, il s'engage à effectuer les corrections ou modifications nécessaires à la mise en sécurité des systèmes et réseaux dans le cadre des exigences du marché.

c. Organisation

Le Titulaire doit désigner au moins une personne en charge des questions de sécurité opérationnelle et doit formellement définir et attribuer les rôles et responsabilités en matière de sécurité au personnel du Titulaire concerné par les applications hébergées au travers du Responsable Sécurité du marché (cf UO\_A6\_3).

d. Protection des données nominatives dans les systèmes d'information de l'application

Toutes les données nominatives stockées ou manipulées par les systèmes d'information du Pouvoir Adjudicateur doivent être protégées afin de garantir la disponibilité, la confidentialité, la traçabilité et l'intégrité des données.

A minima, les règles suivantes s'appliquent :

- Pour le stockage et les sauvegardes, les données doivent être chiffrées ; l'algorithme de chiffrement ainsi que les clés utilisées doivent être conformes aux règles énoncées dans la réglementation en vigueur ;



- Lors du transfert des données, les canaux de communication mis en œuvre doivent garantir la disponibilité, la confidentialité, la traçabilité et l'intégrité des flux ;
- La mise au rebus des équipements ayant stocké ou manipulé des données nominatives fait l'objet d'une démarche d'effacement sécurisé des données en conformité avec la réglementation en vigueur.

#### e. Gestion des droits d'accès

Le Titulaire doit mettre en place des règles et procédures formalisées concernant la gestion des droits d'accès aux différents matériels et logiciels hébergés pour chaque exploitant et administrateur. Ces habilitations doivent systématiquement être tracées, contrôlées et tenues à jour selon les nécessités.

Le Titulaire doit mettre en place une solution de surveillance et de centralisation des accès des utilisateurs avec pouvoirs, conformément à la Politique de sécurité des Systèmes d'information de l'Etat et à la réglementation en vigueur.

#### f. Gestion des incidents de sécurité

Tout incident de sécurité subi par le Titulaire et pouvant avoir des conséquences, avérées ou supposées, sur les actifs du Pouvoir Adjudicateur hébergés par le Titulaire doit être signalé au Pouvoir Adjudicateur dans un délai d'une (1) heure à compter du constat afin qu'il puisse en mesurer l'impact sur son activité et prendre des dispositions d'escalade éventuelles.

Les différents types d'incidents de sécurité seront définis dans le PAS fourni par le Titulaire.

En cas d'incident de sécurité grave ou d'urgence, le Pouvoir Adjudicateur se réserve le droit de requérir l'expertise d'un organisme ou d'une société tierce reconnu pour sa compétence en matière de sécurité. Le Titulaire s'engage à une entière collaboration avec le tiers désigné et à exécuter les consignes prescrites par ce dernier, sous couvert du Pouvoir Adjudicateur.

Un tableau de bord sécurité est produit trimestriellement par le Titulaire.

#### g. Mise à jour de sécurité

Les règles de mise à jour de sécurité et la démarche de mise en œuvre pour l'infrastructure virtuelle (application des correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles, gestion des cas d'alerte grave (attaque virale, faille critique) respecteront les règles annoncées par le CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques).

#### h. Le Plan de Continuité d'Activité

Afin d'assurer un plan de continuité d'activité, le Titulaire dispose d'au moins deux (2) centre de données (datacenters) pour l'hébergement des données et applications confiés par l'ANSM.

Les centres de données du Titulaire hébergeant la part hébergée du système d'information du Pouvoir Adjudicateur sont a minima de niveau Tier III+ (ou équivalent) mais un niveau Tier IV (au sens Uptime Institute) est la cible à privilégier.

Ils doivent être localisés à une distance minimale de plus de trente (30) kilomètres l'un de l'autre.

Le Titulaire s'engage à modifier son plan de continuité si un dysfonctionnement de ce dernier est constaté suite à un exercice ou un incident. Il communiquera au Pouvoir Adjudicateur son plan de continuité modifié dans les meilleurs délais.

#### i. Le Plan d'Assurance Sécurité

Les règles, principes et procédures de sécurité sont repris et détaillés dans un Plan Assurance Sécurité (PAS), s'appuyant sur le Plan de Sécurité du SI du Titulaire qui devient un document contractuel pour la durée de la prestation.

Il constitue un référentiel en termes d'audit sur le management de la sécurité dans le cadre de la prestation assurée par le Titulaire.

Le PAS est finalisé par le Titulaire au cours de la phase de prise en charge avec la participation du Pouvoir Adjudicateur.

Il est soumis pour approbation :

- Au Responsable de Sécurité du système d'information du Pouvoir Adjudicateur,
- Au Comité de Pilotage.

Les évolutions du PAS sont à l'initiative du Titulaire en fonction de son système de gestion des risques. Il doit au minimum procéder à une revue annuelle et réaliser la mise à jour si nécessaire.

Le Titulaire s'assure du respect par ses sous-traitants des exigences de sécurité présentes dans son PAS.

#### j. Comité de Sécurité

Le Titulaire organise un Comité de Sécurité à une fréquence semestrielle.

Ce comité doit permettre d'échanger avec le Pouvoir Adjudicateur sur les sujets de sécurité, notamment l'avancement du plan d'actions sécurité établi lors des comités sécurité précédents, le traitement des incidents de sécurité, l'avancement des travaux de couverture ou de réduction des risques, un bilan des alertes remontées et des correctifs de sécurité installés, un suivi des résultats des audits menés et des plans d'actions associés.

Le Titulaire est en charge de la préparation des Comités : préparation des supports, production d'un tableau de bord de la sécurité. Ce tableau de bord présente a minima la liste des vulnérabilités en cours sur les applications, la liste des incidents de sécurité rencontrés sur le semestre, les travaux de sécurité menés et à venir, et le plan de couverture des risques en cours.

### 4.4. Socle hébergement – exigences générales

#### 4.4.1. Préambule

Cette partie a pour but de décrire les exigences du Pouvoir Adjudicateur sur le plan de l'hébergement des ressources.

Au titre de ses engagements contractuels, le Titulaire fournit une solution d'hébergement pour les systèmes informatiques dont le Pouvoir Adjudicateur a décidé l'externalisation.

L'hébergement des systèmes informatiques est conçu pour viser une continuité de service ininterrompue trois cent soixante-cinq (365) jours par an, vingt-quatre (24) heures sur 24. Il s'entend donc que les infrastructures techniques doivent être maintenues de façon adéquate, d'une part pour prévenir tout incident, mais aussi supporter les interventions planifiées sans pour autant affecter les conditions de production du Pouvoir Adjudicateur.

Les locaux et infrastructures mis à disposition du Pouvoir Adjudicateur par le Titulaire répondent aux normes et réglementations d'hygiène et de sécurité en vigueur, ainsi qu'aux dispositions du code du travail. Le Titulaire s'engage à maintenir la conformité des locaux et moyens mis à disposition du Pouvoir Adjudicateur pendant toute la durée du marché. Si certaines obligations, relevant du périmètre du Titulaire, mettent en jeu la responsabilité du Pouvoir Adjudicateur, le Titulaire s'engage à l'en informer sans délai pour permettre au Pouvoir Adjudicateur de mettre en œuvre les décisions et mesures nécessaires dans les meilleurs délais.

#### 4.4.2. Spécifications générales

##### a. Propriété des sites

Comme indiqué au paragraphe « Règles de sécurité », le Titulaire doit disposer d'au moins deux (2) centres de données (datacenters) géographiquement séparés par une distance minimale de trente (30) kilomètres afin d'assurer son Plan de Continuité d'Activité par la réplication de ses infrastructures techniques.

Le Titulaire doit être soit propriétaire des centres de données soit présenter des garanties de location longue durée qu'il présentera au Pouvoir Adjudicateur sur simple demande de celui-ci.

#### b. Localisation des sites

L'hébergement du système d'information du Pouvoir Adjudicateur doit obligatoirement être localisé sur le territoire français.

Les sites proposés pour l'hébergement ne doivent pas être soumis aux risques majeurs suivants :

- glissement et effondrement de terrain,
- inondation,
- proximité d'une zone de décollage / atterrissage d'un aéroport / aérodrome,
- proximité d'installations Classées pour la Protection de l'Environnement (ICPE) soumises à autorisation,
- proximité d'installations présentant un risque toxique, d'incendie ou d'explosion (en particulier des établissements classés SEVESO).

#### c. Conception et exploitation du centre d'hébergement

L'offre d'hébergement informatique doit répondre aux normes ou aux bonnes pratiques reconnues comme étant des standards de la profession.

Le niveau désiré par le Pouvoir Adjudicateur est *a minima* de type Tier III+ selon la classification de l'Uptime Institute ou équivalent (Type Tier IV à privilégier).

#### d. Alimentation électrique

L'offre d'hébergement doit proposer des conditions d'approvisionnement électrique fiables et correctement dimensionnées au regard de son offre de service.

#### e. Régulation en température des locaux techniques et salles informatiques

L'offre d'hébergement doit assurer une température régulée et conforme aux prescriptions des constructeurs de matériels informatiques.

#### f. Détection d'eau

Les locaux mis à disposition pour la réalisation des prestations sont équipés de dispositifs de détection d'eau installés dans les faux planchers informatiques.

#### g. Détection incendie

L'ensemble des locaux sont dotés de dispositifs de détection et d'extinction d'incendie, selon la réglementation en vigueur.

Les salles informatiques et de télécommunication sont équipées de systèmes automatiques d'extinction d'incendie, répondant aux normes relatives à la sécurité des personnes, et dont l'emploi est non destructif pour les matériels hébergés.

#### h. Sécurité d'accès physique

Les locaux prévus pour l'exécution du marché sont parfaitement sécurisés et disposent des moyens aptes à prévenir toute intrusion physique.

#### i. Procédure d'accès aux locaux

Les accès du personnel du Titulaire, des tiers mainteneurs, des visiteurs divers sur les différentes zones sont soumis à des procédures de délivrance des autorisations d'accès.

j. Entretien des installations entrant dans la fourniture des services délivrés au Pouvoir Adjudicateur

---

Les installations font l'objet d'un entretien et de contrôles réguliers, effectués par des mainteneurs et organismes compétents et ce niveau de qualité de service est maintenu durant toute la durée du marché.

k. Démarche environnementale du Titulaire

---

Le Titulaire suit une politique en matière de sauvegarde de l'environnement par la mise en place de dispositions et par des investissements visant à réduire la consommation énergétique, l'émission de gaz à effet de serre et en eau, ainsi que l'impact sur l'environnement de ses activités. Il met en œuvre les engagements pris dans son offre conformément au CCAP.

#### 4.4.3. Prestations attendues de service régulier

---

Les prestations à fournir pour la phase de service régulier couvrent les activités suivantes :

- la surveillance 24 heures sur 24, 7 jours sur 7 du datacenter (avec contrôle de l'accès physique, de l'alimentation électrique, de la climatisation, accompagnement des personnels désignés par le Pouvoir Adjudicateur pour intervenir sur ses ressources ...) ;
- la gestion courante des infrastructures d'hébergement :
  - l'exploitation, la supervision en temps réel, l'administration et le maintien en conditions opérationnelles des infrastructures physiques d'hébergement et des infrastructures informatiques du Datacenter (nettoyage des locaux, entretien et maintenance du système de climatisation, des installations électriques,...)
  - les visites régulières de contrôle des espaces physiques d'hébergement. Les moyens de prévention et de protection mis en place doivent faire l'objet de maintenances et de contrôles réguliers.

#### 4.4.4. Engagements et niveaux de service

---

Les niveaux de services et les engagements associés sont précisés dans la convention de service (annexe 2 du CCTP).

#### 4.4.5. Modèle Financier

---

Les prestations liées à ce module ne font pas l'objet d'unités d'œuvre dédiées. Le coût lié est compris dans les unités d'œuvres des modules suivants.

### 4.5. Module A1 – Support aux utilisateurs

---

#### 4.5.1. Périmètre

---

Les utilisateurs de ce module sont les équipes du Pouvoir Adjudicateur.

La liste des utilisateurs autorisés à utiliser le support aux utilisateurs sera communiquée au Titulaire au démarrage du marché. Cette liste pourra être mise à jour régulièrement en cours de marché.

La liste des interlocuteurs à prévenir en cas d'incident (voir définition ci-après) détecté par le Titulaire sera également communiquée au démarrage du marché et pourra être mise à jour tout au long du marché.

#### 4.5.2. Définitions

---

Les sollicitations du guichet de production fourni par le Titulaire sont de deux (2) types :

1. Les incidents
2. Les demandes.

### **Les incidents :**

Un incident est un évènement qui vient perturber le bon fonctionnement des services hébergés par le Titulaire. On entend par service l'ensemble des fonctionnalités et prestations d'hébergement, et la documentation afférente.

Un incident survient par définition de façon aléatoire à n'importe quel moment (heures ouvrées et non ouvrées).

Au titre des prestations des modules A2 à A5, le Titulaire est amené à détecter et traiter des incidents.

Le Pouvoir Adjudicateur peut aussi être amené à signaler l'existence d'un incident au Titulaire. Le support aux utilisateurs a pour fonction de recueillir et traiter ces signalements d'incidents et d'informer, en permettant la consultation directe par le Pouvoir Adjudicateur de l'outil de suivi des incidents de leur évolution et traitement.

Dans le cas d'un signalement par le Pouvoir Adjudicateur, les incidents reçus par le Titulaire auront donc déjà fait l'objet d'une classification par le Pouvoir Adjudicateur.

Les types d'incident potentiels sont classés par niveau de criticité :

- Bloquant / généralisé : Service interrompu. Concerne l'ensemble des utilisateurs du service. Il n'existe pas de solution de contournement immédiate.
- Dégradé : Incident soit avec un service dégradé sans rupture, soit rupture avec solution de contournement existante. Concerne plusieurs utilisateurs du service.
- Mineur : Incident unitaire, rupture ou dégradation du service pour un seul utilisateur. Correction ou solutions de contournement accessibles immédiatement.

Le délai maximum d'information des incidents bloquants est de quinze (15) minutes.

Il est attendu du Titulaire qu'il soit force de proposition et d'action quant à l'amélioration continue du dispositif opéré, notamment par une analyse causale des incidents rencontrés, et leur éventuel classement / traitement en tant que problèmes.

### **Les demandes :**

Les demandes constituent toutes les autres sollicitations (qui ne sont pas des incidents) que le Pouvoir Adjudicateur soumet au Titulaire dans le cadre de l'hébergement des services.

Exemples de demandes (liste non exhaustive) :

- Demande de restauration ou sauvegarde ponctuelle de n'importe quel élément,
- Demande de passage d'un batch ponctuel,
- Demande de rafraichissement d'environnement,
- Création d'un nom de domaine,
- Fourniture d'un certificat SSL mono site/multi site conforme à la réglementation en vigueur...

#### **4.5.3.Détail des prestations attendues**

Les services attendus, doivent couvrir les aspects de centre d'appels et d'assistance et support de niveau 1 et 2.

Il est entendu par niveaux d'assistance :

- Niveau 1 : Hotline – Centre d'appels, pour la qualification et la résolution sur procédures des incidents et demandes mineures ;
- Niveau 2 : Technicien, pour la résolution des problèmes, des incidents et demandes non résolus au niveau 1.

Les demandes et les incidents peuvent être soumis au Titulaire soit par téléphone (avec une intégration après dans l'interface par le Titulaire) soit par une interface Web de saisie des demandes et des

incidents (outil de création et de suivi des tickets). Le Titulaire a pour obligation de proposer ces deux (2) modes d'accueil en parallèle. Le Titulaire précisera les modalités de fonctionnement proposées.

- La création des tickets comprend a minima : la qualification d'impact / gravité d'un incident qui devra être systématiquement validée par le demandeur (de l'équipe du Pouvoir Adjudicateur).

Le traitement comprend a minima (fonction d'assistance et support) :

- diagnostic direct sur base de consignes ou de procédures écrites ;
- escalade et routage des dossiers vers les équipes de support de niveau supérieur, internes du Titulaire ou du Pouvoir Adjudicateur, quand cela est nécessaire ;
- suivi de bout en bout des dossiers en cours ;
- escalade hiérarchique immédiate en cas d'incident bloquant ou généralisé ;
- communication auprès des relais identifiés au Pouvoir Adjudicateur.

Le Titulaire a pour obligation de communiquer l'avancement du traitement du ticket au fur et à mesure de son avancement. La résolution d'un incident doit être toujours notifiée au demandeur.

La matrice de communication et la procédure de gestion de crise sont définies conjointement pendant la phase de transition.

Un ticket est considéré clos à partir du moment où le service est réputé rendu et que cela est consigné dans l'outil de suivi. Cette notion de clôture peut être invalidée par le demandeur, le ticket est alors ré-ouvert et réattribué à un groupe de résolution, le délai pour suivi des indicateurs de performance continuant de s'écouler.

La clôture du ticket donne lieu à explications dans l'outil de gestion des incidents. Ces explications doivent permettre au Pouvoir Adjudicateur d'apprécier la bonne résolution de l'incident et sa clôture effective.

Le suivi comprend a minima la mise à jour et l'accessibilité du référentiel documentaire (consignes, modes opératoires,...).

### **Procédure d'escalade**

La procédure d'escalade est mise en œuvre par le Titulaire en cas d'interruption significative ou de dysfonctionnement grave.

Cette procédure vise à avertir les différents responsables du Pouvoir Adjudicateur et du Titulaire lors d'un dysfonctionnement des opérations, ou lors d'interruptions graves (comme un serveur hors fonction, une attaque virale, un réseau inopérant) non résolu.

La procédure d'escalade est enclenchée en cas d'échec de la résolution de l'incident dans le respect de la GTR indiquée dans la convention de services.

La procédure d'escalade n'a pas d'incidence sur le calcul du montant des pénalités qui commencent à courir à compter du dépassement de la GTI et/ou de la GTR même en cas de mise en œuvre de cette procédure, ni sur celui du calcul des indicateurs de qualité de service (conformément à la convention de service).

Les grands principes d'escalade sont les suivants :

#### **a) L'escalade :**

Cette phase consiste à initialiser toutes les actions nécessaires à la résolution de l'incident et, par là-même, à prévenir toutes les entités impliquées et coordonner leur action.

#### **b) La correction :**

Une fois le plan d'action de correction identifié et préparé par le Titulaire, le service concerné du Titulaire informe le correspondant du Pouvoir Adjudicateur pour validation par celui-ci de la décision d'appliquer ce plan.

c) La cellule de crise :

En cas d'insuccès du plan d'action, le correspondant du Pouvoir Adjudicateur et le service concerné du Titulaire conviennent de déclencher une cellule de crise opérationnelle jusqu'à la résolution de l'incident. Les participants à cette cellule sont nommés par le correspondant du Pouvoir Adjudicateur et le service concerné du Titulaire. Cette cellule de crise établit un reporting quotidien de l'évolution de la situation.

d) Le retour en situation normale :

Une fois la correction appliquée, après un temps d'observation du fonctionnement du service de façon normale (la durée de cette période d'observation est précisée dans le plan d'action), le service concerné du Titulaire informe le correspondant du Pouvoir Adjudicateur du retour à la normale. Il prépare un compte rendu sur l'incident pour présentation au comité de pilotage.

#### 4.5.4. Engagements et niveaux de services

---

Le Titulaire doit organiser le support aux utilisateurs de façon à être en mesure d'accueillir :

- Des demandes pendant les plages d'heures ouvrées ;
- Les remontés d'incidents / la communication en H24 (soit 24 heures sur 24) pour escalade à des référents désignés par le Pouvoir Adjudicateur pour les dispositifs critiques. Pour les heures non ouvrées, un système d'astreinte est mis en place.

#### 4.5.5. Modèle Financier

---

Les prestations liées à ce module ne font pas l'objet d'unités d'œuvre dédiées. Le coût lié est compris dans les unités d'œuvre des modules suivants.

### 4.6. Module A2 – Fourniture d'une connexion Internet

---

#### 4.6.1. Périmètre Technique

---

Le périmètre technique de ce module couvre la fourniture d'une connexion internet et la fourniture d'un tunnel VPN :

a. La connexion internet

---

- Est délivrée par un/des lien(s) physique(s) fibre(s) opérateur(s) ;
- Est résistante au risque « perte d'un site » et au risque « perte d'un backbone d'un provider » ;
- Est fournie avec les équipements de sécurité (FW, WAF, IDP/IPS) mutualisés conformes aux règles de l'art avec les services de maintien en condition opérationnelle (MCO) inclus dans le loyer mensuel ;
- Permet au Pouvoir Adjudicateur de dimensionner le débit offert en fonction de tranches de débits proposées ;
- Offre une bande passante garantie et flexible afin de garantir des bons temps de réponse. Cette bande passante peut évoluer progressivement en fonction des besoins du Pouvoir Adjudicateur et en fonction de la progression de l'audience des applications.
- Propose :
  - un service de filtrage (FW et WAF) suivant les besoins du Pouvoir Adjudicateur,
  - un service de LoadBalancing,
  - un service Anti DDoS.

b. Le tunnel VPN

---

Une liaison sécurisée permanente VPN (IPsec) est proposée pour permettre au Pouvoir Adjudicateur :

- d'administrer ses VM en mode IaaS ;
- d'accéder au LDAP, au serveur SMTP et à des bases de données de l'ANSM ;
- d'interconnecter les services hébergés avec son site principal.



Par défaut, une solution VPN IPsec (avec chiffrement AES-256, authentification forte et tunnel redondé) est attendue. Cependant, le Titulaire peut proposer, en alternative ou en complément, d'autres technologies équivalentes ou supérieures en termes de sécurité et de performance, telles que :

- Une liaison MPLS (avec garantie de QoS et isolation du trafic),
- Un accès dédié (type Ethernet privé ou lien optique),
- Une solution SD-WAN (pour une gestion dynamique des flux),
- Ou toute autre technologie validée par le Pouvoir Adjudicateur, sous réserve qu'elle réponde aux exigences suivantes :
  - Chiffrement des flux (norme FIPS 140-2 ou équivalente),
  - Disponibilité minimale de 99,9 %,
  - Redondance des liens (pour éviter les points de défaillance uniques),
  - Compatibilité avec les infrastructures existantes du Pouvoir Adjudicateur.

Le Titulaire aura détaillé sa proposition technique dans son offre, en précisant :

- Le type de liaison proposé (VPN, MPLS, SD-WAN, etc.),
- Les performances garanties (bande passante, latence),
- Les modalités de supervision et de maintenance.

#### 4.6.2. Prestations attendues

---

N.B. : les unités d'œuvres (UO) en face de chaque ensemble de prestations, font références aux unités d'œuvre du BPU.

Les prestations à fournir couvrent les activités suivantes:

- UO\_A2\_1\_S : les services de mise en place d'une connexion internet (frais de setup) ;
- UO\_A2\_1 : les services de maintien de la connexion internet (loyer mensuel) avec :
  - ✓ relation avec l'opérateur (intervention et maintenance),
  - ✓ surveillance du service 24h/24, 7j/7,
  - ✓ mise à disposition des statistiques d'accès et d'utilisation (bande passante, ...) accessibles en ligne,
  - ✓ Protection anti-DDoS standard : coupure du site en cas d'attaque DDos ;
- UO\_A2\_2\_S : Mise en place d'un Tunnel VPN (frais de setup) ;
- UO\_A2\_2 : les services de maintien d'un tunnel VPN (loyer mensuel) avec :
  - ✓ surveillance du service 24h/24, 7j/7,
  - ✓ mise à disposition des statistiques d'accès et d'utilisation (bande passante, ...) accessibles en ligne,
  - ✓ mise en place des règles de flux ;
- UO\_A2\_3\_S : Mise en place de la Mutualisation de charge (LoadBalancing) (frais de setup) ;
- UO\_A2\_3 : Gestion des règles de la mutualisation de charge (LoadBalancing) (loyer mensuel) ;
- UO\_A2\_4\_S : Déclaration et configuration des adresses IP ;
- UO\_A2\_5\_S : Installation d'une Protection anti-DDoS avancée permettant de maintenir l'accès et le trafic sur le site pendant l'attaque ;
- UO\_A2\_5 : Gestion de l'anti-DDoS : analyse des flux, détection des menaces, remontée des alertes au Pouvoir Adjudicateur, activation de la protection ;
- UO\_A2\_6\_S : Installation et configuration de Firewall, WAF et IPS/IDS ;
- UO\_A2\_6 : Gestion des règles de filtrage, supervision, remontée des alertes au Pouvoir Adjudicateur ;
- UO\_A2\_7\_S et UO\_A2\_8\_S : Certificat SSL avec :
  - L'installation et l'abonnement du certificat SSL mono-site ou multi-site ;
- UO\_A2\_9\_S : Mise en place du service de cache ;
- UO\_A2\_9 : Gestion des règles du service de cache ;
- UO\_A2\_10\_S : Mise en place d'un web application Firewall ;
- UO\_A2\_10 : Gestion des règles du web application Firewall.

Le Pouvoir Adjudicateur administre entièrement ses domaines (registrar et adresse IP comprises).

#### 4.6.3. Engagements et niveaux de service

---

Les niveaux de services et les engagements associés sont décrits dans la convention de services (annexe 2 du CCTP).

Le Titulaire s'engage à fournir pour la connexion internet :

- une disponibilité mensuelle minimum supérieure au niveau indiqué dans la convention de services, avec prise en compte du risque « perte d'un site » et « perte du backbone d'un provider » ;
- un débit minimum de 100Mb/s garanti ;
- une garantie de la reprise des IP en cas de perte d'un site ou d'un équipement de la chaîne d'accès ;
- un trafic illimité.

Il est entendu que ces engagements se mesurent « au plus près » des ressources du Pouvoir Adjudicateur. Le Titulaire est tenu responsable si des engagements de disponibilité ou de qualité de service non tenus sont induits par des incidents / problèmes au sein du Datacenter.

#### 4.6.4. Outillage de service

---

Au titre de la prestation, est compris l'outillage de surveillance de la connexion.

La mise à disposition de l'outillage de service ne fait pas l'objet d'un surcoût dédié. Le coût lié à la mise à disposition est compris dans les unités d'œuvres du module.

#### 4.6.5. Modèle Financier

---

Les prestations du module sont rémunérées conformément aux UO du BPU.

### 4.7. Module A3.1 - Fourniture de capacités de type Infrastructure virtuelle

---

#### 4.7.1. Préambule

---

Ce module a pour finalité la fourniture, la mise à disposition de capacités (serveurs virtuels, espaces de stockage, dispositifs de sauvegarde...) et des infrastructures les supportant :

- dispositifs techniques sous la responsabilité du Titulaire (réseau, serveurs physiques, stockage, OS ...) installés par le Titulaire ;
- l'hébergement de ces dispositifs.

La fourniture, la supervision, l'exploitation et l'administration des infrastructures physiques d'hébergement (électricité, climatisation, protection incendie, contrôle d'accès, ...) et des infrastructures informatiques (câbles réseau, dispositifs de sécurité,...) liées aux capacités sont dans le périmètre de ce module et sous la responsabilité du Titulaire.

La supervision, l'exploitation et l'administration des dispositifs techniques et applicatifs qui sont installés par le Pouvoir Adjudicateur sur les capacités fournies n'entrent pas dans les prestations attendues du Titulaire dans le périmètre de ce module.

#### 4.7.2. Périmètre Technique

---

Les capacités sont fournies selon les besoins du Pouvoir Adjudicateur en infrastructure virtuelle correspondant à un ensemble d'infrastructures fournies comme des services, supportées par des ressources matérielles dédiées (switch réseau dédié, serveurs dédiés, stockage dédié, ...), fonctionnant pour une organisation unique et gérée par le Titulaire (intégrant les activités de supervision, maintenance, exploitation ...)

Le Titulaire dispose d'une infrastructure informatique lui permettant de fournir les ressources système, réseau et sécurité en fonction des besoins exprimés par le Pouvoir Adjudicateur.

Les serveurs virtuels mis à disposition présentent une complète compatibilité (engagement de support de l'éditeur de la solution de virtualisation), pour les systèmes d'exploitation et applicatifs suivants, dans les versions supportées par les éditeurs :

- Microsoft Windows server,
- Microsoft SQL server / MySQL / SQLite / PostgreSQL / ORACLE / MongoDB / ElasticSearch,
- Linux Debian, CentOS, RedHat & Suse,
- Conteneurs Docker / Orchestrateur Kubernetes / Automatisme Ansible Engine,
- Apache / NGINX / IIS,
- JBoss / Tomcat,
- PHP/.Net/Python/Java,
- Varnish, HAProxy / Memcached.

Les capacités fournies par le titulaire sont des VM avec stockage associé en mode infrastructure virtuelle.

La grille de dimensionnement du socle infrastructure virtuelle comprend tous les dispositifs sous-jacents (redondance serveurs N+1, serveurs multi-site, licences hyperviseur...) à l'infrastructure virtuelle.

Il est ainsi mis à disposition du Pouvoir Adjudicateur des VM dont il est possible de moduler les critères suivants :

- nombre de processeurs virtuels ou équivalent reflétant la puissance de calcul,
- quantité de mémoire vive allouée au serveur virtuel,
- volume de l'espace disque alloué au serveur virtuel.

Le Pouvoir Adjudicateur propose la granularité suivante :

- processeurs virtuels comptés à l'unité,
- mémoire vive par tranche de quatre gigaoctets (4 Go),
- espace disque par tranche de cent gigaoctets (100 Go).

Classes de services :

Les classes de services attendues pour l'infrastructure virtuelle dédiée sont les suivantes :

- Classe standard :
  - taux de disponibilité des machines virtuelles : 99,9%,
  - disponibilité du service 24/24, 7/7,
  - Plage de service garantie : 24/24, 7/7,
- Classe haute performance :
  - Les taux de disponibilité des machines virtuelles et du stockage seront supérieurs à 99,98%,
  - Niveau de performance élevé : hébergement d'applications hautement consommatrices de ressources (CPU, RAM, espace disque),
  - Evolutivité horizontale : adaptation rapide et souple par ajout de ressources en prévision des pics de trafic (ressources hardware, clusterisation, auto scale up, load balancing).

Le Titulaire précise les frais de mise en place (frais setup) et le loyer mensuel dans le cadre de données HDS et de données non-HDS.

#### 4.7.3.Détail des prestations attendues

N.B. : les unités d'œuvres (UO) en face de chaque ensemble de prestations, font références aux unités d'œuvre du BPU.

- a. UO\_A3.1\_1\_S à UO\_A3.1\_5\_S et  
UO\_A3.1\_1 à UO\_A3.1\_5 et  
UO\_A3.1\_1\_S\_HDS à UO\_A3.1\_5\_S\_HDS et  
UO\_A3.1\_1\_HDS à UO\_A3.1\_5\_HDS : Fourniture de capacités en infrastructure virtuelle (Classe standard)

Fourniture de VM et ajout de capacité de vCPU, de vRAM et de stockage supplémentaire en infrastructure virtuelle suivant le niveau attendu en classe standard.

L'hébergement de ces capacités fournies inclut l'intégralité des prestations attendues au socle hébergement (article 4.4 du présent CCTP).

- b. UO\_A3.1\_6\_S à UO\_A3.1\_10\_S et  
UO\_A3.1\_6 à UO\_A3.1\_10 et  
UO\_A3.1\_6\_S\_HDS à UO\_A3.1\_10\_S\_HDS et  
UO\_A3.1\_6\_HDS à UO\_A3.1\_10\_HDS : Fourniture de capacités en infrastructure virtuelle (Classe haute performance)

Fourniture de VM et ajout de capacité de vCPU, de vRAM et de stockage supplémentaire en infrastructure virtuelle suivant le niveau attendu en classe haute performance.

L'hébergement de ces capacités fournies inclut l'intégralité des prestations attendues au socle hébergement (article 4.4 du présent CCTP).

- c. UO\_A3.1\_11\_S et UO\_A3.1\_11 et UO\_A3.1\_11\_S\_HDS et UO\_A3.1\_11\_HDS :  
Stockage partagé

Fourniture d'espace de stockage NAS.

L'hébergement de ces capacités fournies inclut l'intégralité des prestations attendues au socle hébergement (article 4.4 du présent CCTP).

- d. UO\_A3.1\_12\_S à UO\_A3.1\_15\_S et  
UO\_A3.1\_12 à UO\_A3.1\_15 et  
UO\_A3.1\_12\_S\_HDS à UO\_A3.1\_15\_S\_HDS et  
UO\_A3.1\_12\_HDS à UO\_A3.1\_15\_HDS : Fourniture de licences en infrastructure virtuelle

Fourniture de licences OS et DB en infrastructure virtuelle : Installation (frais de setup) et utilisation (loyer mensuel).

#### 4.7.4.Engagements et niveaux de service

Le Titulaire s'engage à :

- accepter des audits (réalisés par le Pouvoir Adjudicateur ou par un tiers) sur les infrastructures (stockage, réseau, virtualisation, ...) supportant les infrastructures mises à disposition du Pouvoir Adjudicateur (ex : contrôler que l'infrastructure virtuelle est bien conforme "à l'état de l'art", qu'elle est performante, contrôler que les ratios de consolidation sur l'infrastructure virtuelle sont inférieurs aux seuils préconisés, ...) sur demande du Pouvoir Adjudicateur conformément aux stipulations du CCAP ;
- informer le Pouvoir Adjudicateur (avant la réalisation des opérations - 10 jours ouvrés avant minimum) dès qu'il y a des mises à jour (patch sur les baies, montées de version sur la virtualisation, ...) sur les dispositifs techniques de l'infrastructure virtuelle qui supporte le système d'information du Pouvoir Adjudicateur ; le Pouvoir Adjudicateur doit pouvoir demander une re-planification des mises à jour ;
- disposer de générations de matériels (moins de 4 ans) et logiciels récentes (moins de 2 ans) à la mise en service.

Les classes de services des capacités fournies sont précisées au chapitre 4.6.2.

Les engagements sont précisés dans la convention de services (annexe 2 du CCTP).

#### 4.7.5.Outillage de services

Le Titulaire doit disposer d'outils de surveillance pour la supervision, l'exploitation et l'administration des équipements (création / modification de VM, création / modification d'espace de stockage, récupération de sauvegarde, restauration de données..).

Cet outillage permet de produire les alertes et les indicateurs de niveaux de services demandés conformément à la convention de services.

Ces outils doivent dans la mesure du possible être accessibles au Pouvoir Adjudicateur.

La mise à disposition de l'outillage de service ne fait pas l'objet d'un surcoût dédié. Le coût lié à la mise à disposition est compris dans les UO du module.

#### 4.7.6. Modèle Financier

---

Les prestations du module sont rémunérées conformément aux UO du BPU.

### 4.8. Module A3.2 - Fourniture de serveurs physiques

---

#### 4.8.1. Préambule

---

Ce module a pour finalité la fourniture, la mise à disposition de serveurs physiques et des infrastructures les supportant :

- dispositifs techniques sous la responsabilité du Titulaire (réseau, stockage, OS ...) installés par le Titulaire ;
- l'hébergement de ces dispositifs.

La fourniture, la supervision, l'exploitation et l'administration des infrastructures physiques d'hébergement (électricité, climatisation, protection incendie, contrôle d'accès, ...) et des infrastructures informatiques (câbles réseau, dispositifs de sécurité,...) liées aux capacités sont dans le périmètre de ce module et sous la responsabilité du Titulaire.

La supervision, l'exploitation et l'administration des dispositifs techniques et applicatifs qui seront installés par le Pouvoir Adjudicateur sur les capacités fournies n'entrent pas dans les prestations attendues du Titulaire dans le périmètre de ce module.

#### 4.8.2. Périmètre Technique

---

Le Titulaire dispose d'une infrastructure informatique lui permettant de fournir les ressources système, réseau et sécurité en fonction des besoins exprimés par le Pouvoir Adjudicateur.

Les serveurs virtuels mis à disposition présentent une complète compatibilité (engagement de support de l'éditeur de la solution de virtualisation), pour les systèmes d'exploitation et applicatifs suivants, dans les versions supportées par les éditeurs :

- Microsoft Windows server,
- Microsoft SQL server / MySQL / SQLite / PostgreSQL / ORACLE / MongoDB / ElasticSearch,
- Linux Debian, CentOS, RedHat & Suse,
- Conteneurs Docker / Orchestrateur Kubernetes / Automatismes Ansible Engine,
- Apache / NGINX / IIS,
- JBoss / Tomcat,
- PHP/.Net/Python/Java,
- Varnish, HAProxy / Memcached.

Le Titulaire précise les frais de mise en place (frais setup) et le loyer mensuel dans le cadre de données HDS et de données non-HDS.

#### 4.8.3. Détail des prestations attendues

---

N.B. : les UO en face de chaque ensemble de prestations, font références aux unités d'œuvre du BPU.

- a. UO\_A3.2\_1\_S à UO\_A3.2\_2\_S et  
UO\_A3.2\_1 à UO\_A3.2\_2 et  
UO\_A3.2\_1\_S\_HDS à UO\_A3.2\_2\_S\_HDS et  
UO\_A3.2\_1\_HDS à UO\_A3.2\_2\_HDS :  
Fourniture de serveurs physiques dédiés
- 

Fourniture de serveurs physiques.

L'hébergement de ces capacités fournies inclut l'intégralité des prestations attendues au module A1 socle hébergement : infrastructure d'hébergement et informatique.

- b. UO\_A3.2\_3\_S et UO\_A3.2\_3 et UO\_A3.2\_3\_S\_HDS et UO\_A3.2\_3\_HDS :  
Stockage partagé
- 

Fourniture d'espace de stockage NAS.

L'hébergement de ces capacités fournies inclut l'intégralité des prestations attendues au socle hébergement (article 4.4 du présent CCTP).

- c. UO\_A3.2\_4\_S à UO\_A3.2\_7\_S et  
UO\_A3.2\_4 à UO\_A3.2\_7 et  
UO\_A3.2\_4\_S\_HDS à UO\_A3.2\_7\_S\_HDS et  
UO\_A3.2\_4\_HDS à UO\_A3.2\_7\_HDS :  
Fourniture de licences sur serveurs physiques
- 

Fourniture de licences OS et DB : Installation (frais de setup) et utilisation (loyer mensuel).

#### 4.8.4. Engagements et niveaux de service

---

Le Titulaire s'engage :

- à accepter des audits (réalisés par le Pouvoir Adjudicateur ou par un tiers) sur les infrastructures (stockage, réseau, virtualisation, ...) supportant les infrastructures mises à disposition du Pouvoir Adjudicateur (ex : contrôler que l'infrastructure virtuelle est bien conforme "à l'état de l'art", qu'elle est performante, contrôler que les ratios de consolidation sur l'infrastructure virtuelle sont inférieurs aux seuils préconisés, ...) sur demande du Pouvoir Adjudicateur conformément aux stipulations du CCAP.
- à disposer de générations de matériels (moins de 4 ans) et logiciels récentes (moins de 2 ans) à la mise en service.

Les engagements sont précisés dans la convention de services (annexe 2 du CCTP).

#### 4.8.5. Outillage de services

---

Le Titulaire doit disposer d'outils de surveillance pour la supervision, l'exploitation et l'administration des équipements (création / modification de VM, création / modification d'espace de stockage, récupération de sauvegarde, restauration de données..).

Cet outillage permet de produire les indicateurs de qualité de service demandés conformément à la convention de services et les alertes.

Ces outils doivent dans la mesure du possible être accessibles au Pouvoir Adjudicateur.

La mise à disposition de l'outillage de service ne fait pas l'objet d'un surcoût dédié. Le coût lié à la mise à disposition est compris dans les unités d'œuvres du module.

#### 4.8.6. Modèle Financier

---

Les prestations du module sont rémunérées conformément aux UO du BPU.

### 4.9. Module A4 – Service d'infogérance et prestations de service associé

---

#### 4.9.1. Préambule

---

Ce module a pour finalité la description des services d'infogérance et prestations de service associées attendues.

#### 4.9.2. Périmètre technique

Les prestations à fournir pour la phase de service régulier couvrent les activités d'initialisation du service, de supervision, d'exploitation courantes et d'administration quotidienne des dispositifs techniques.

Quatre (4) types de prestations sont possibles : OS, WEB, FRONT, BDD.

Les UO peuvent concerner des capacités HDS, c'est-à-dire prenant en compte les infrastructures nécessaires à l'hébergement de données de santé. Les noms de ces UO se terminent par « \_HDS ».

Deux (2) classes de service sont attendues :

- Classe haute performance principalement pour les serveurs / VM de production, 7j/7, 24h/24 ;
- Classe standard principalement pour les serveurs de pré-production, 7j/7, de 9h00 à 18h00.

Voici une liste non exhaustive de demandes de prestations d'infogérance :

Base de données : Application d'un patch à la demande
Base de données : Backup d'une base à la demande
Base de données : Création de base de données (manuelle, via script ou import)
Base de données : Création d'une table (manuelle, via script ou import)
Base de données : Défragmentation d'une base
Base de données : Déplacement d'une table space
Base de données : Migration de base de données
Base de données : Mise à disposition des requêtes lentes ou traces à la demande
Base de données : Mise en place d'un plan de sauvegarde
Base de données : Mise en place d'une synchronisation entre bases
Base de données : Mise en place d'une tâche planifiée
Base de données : Modification de droit utilisateur
Base de données : Modification d'un paramètre du moteur de base de données
Base de données : Passage d'un script CLIENT en base
Base de données : Relance d'une instance de base de données à la demande
Base de données : Restauration d'une base à la demande
Arrêt / Démarrage d'une machine virtuelle
Changement de mot de passe outil interne
Création d'un modèle de machine virtuelle
Modification de configuration d'une machine virtuelle
Redémarrage d'un équipement à la demande
Conversion d'une machine virtuelle en physique (V2P)
Conversion d'une machine physique en virtuelle (P2V)
Programmation / Planification du déploiement manuel ou automatique d'une machine virtuelle
Sauvegarde : Restauration à la demande d'un support mensuel/annuel fourni préalablement à l'ANSM
Sauvegarde : Fourniture d'un support mensuel à l'ANSM pour conservation annuelle ou définitive.
Sauvegarde : Mise en place de la rotation et réalisation de la sauvegarde d'une machine virtuelle.
Sauvegarde : Mise en place de la rotation et réalisation de la sauvegarde d'un conteneur
Sauvegarde : Mise en place de la rotation et réalisation de la sauvegarde d'une application
Sauvegarde : Mise en place de la rotation et réalisation de la sauvegarde d'une base de données
Réseau : Ajout d'une Ip publique
Réseau : Ajout d'une nouvelle IP de répartition de charge (load balancing)



Réseau : Ajout d'une route statique
Réseau : Ajout/modification d'enregistrement DNS gérés par PRESTATAIRE (sous-domaine PRESTATAIRE) (par enregistrement)
Réseau : Création/Modification de VLAN (par VLAN)
Réseau : Déplacement physique d'un équipement (Switch, serveur, LB, Firewall)
Réseau : Modification de configuration d'une ou plusieurs interfaces réseau sur un serveur
Réseau : Modification du filtrage machine (Iptable)
Réseau : Modification d'une ferme de répartition de charge (load balancing)
Réseau : Modification/ajout de règle firewall (par demande)
Linux : Ajout de module apache (php etc..) (par module)
Linux : Ajout script rotation de logs
Linux : Création de compte ftp
Linux : Création d'un point de montage de type NFS ou CIFS (exemple SAN)
Linux : Création d'utilisateur
Linux : Installation Apache
Linux : Installation du service FTP
Linux : Installation d'un antivirus
Linux : Installation d'un patch applicatif à la demande du CLIENT
Linux : Installation d'un script de synchronisation de fichiers de type rsync
Linux : Installation d'une clef SSL
Linux : Mise à jour du Kernel
Linux : Modification de droits sur fichier/répertoire
Linux : Modification de la liste des tâches planifiées (crontab)
Linux : Modification de l'espace de stockage (SAN, NAS, NFS etc..)
Linux : Modification de paramètre Apache / Tomcat / NGINX
Linux : Ajout, redémarrage, modification, arrêt d'un conteneur Docker
Linux : Programmation / Planification du déploiement manuel ou automatique de conteneurs
Linux : Modification du fichier php.ini
Linux : Redémarrage de serveur à la demande avec suivi de procédure CLIENT
Linux : Relance de service à la demande avec suivi de procédure CLIENT
Linux : Renouvellement du certificat SSL
Linux : Restauration d'un backup à la demande du CLIENT
Windows : Ajout script rotation de logs
Windows : Création de compte ftp
Windows : Création d'un point de montage (Volume) de type NTFS ou CIFS (exemple SAN)
Windows : Création d'utilisateur
Windows : Installation de composant IIS
Windows : Installation du service FTP
Windows : Installation d'un antivirus
Windows : Installation d'un patch applicatif à la demande du CLIENT
Windows : Installation d'un script de synchronisation de fichiers de type robocopy
Windows : Installation d'une clef SSL
Windows : Installation IIS
Windows : Mise à jour d'une version majeure d'un applicatif (Apache, Tomcat, etc...)
Windows : Modification de droits sur fichier/répertoire

Windows : Modification de la liste des tâches planifiées (MS)
Windows : Modification de l'espace de stockage (SAN, NAS, NFS etc..)
Windows : Modification de paramètre IIS
Windows : Rattachement d'un serveur dans un Active Directory
Windows : Redémarrage de serveur à la demande avec suivi de procédure CLIENT
Windows : Relance de service à la demande avec suivi de procédure CLIENT
Windows : Renouvellement du certificat SSL
Windows : Restauration d'un backup à la demande du CLIENT
Windows : Ajout, redémarrage, modification, arrêt d'un conteneur Docker

A cette liste viennent s'ajouter les demandes complémentaires pour lesquelles le Titulaire s'est engagé contractuellement.

#### 4.9.3. Détail des prestations attendues

N.B. : les UO en face de chaque ensemble de prestations font références aux unités d'œuvre du BPU.

- a. UO\_A4\_1\_S à UO\_A4\_8\_S et UO\_A4\_1\_S\_HDS à UO\_A4\_8\_S\_HDS:  
Initialisation

L'initialisation du service comprend :

- la mise en place des outils de supervision pour la supervision technique,
- la création des consignes, arbres de décisions et d'escalades par le Titulaire pour la supervision des dispositifs techniques,
- la mise en place des procédures d'exploitation, de backup et d'administration pour les dispositifs techniques,
- la fourniture des outils et documents associés à l'exploitation et l'administration des dispositifs techniques.

- b. UO\_A4\_1 à UO\_A4\_8 et UO\_A4\_1\_HDS à UO\_A4\_8\_HDS : Supervision,  
exploitation et administration

#### → **Supervision des dispositifs techniques :**

Le Titulaire assure :

- le contrôle de la disponibilité des dispositifs surveillés,
- l'exécution des opérations récurrentes consignées de production (réinitialisation de serveur, ...),
- la surveillance en particulier des espaces de stockage (vérification de leur intégrité, suivi des taux d'occupation par rapport à l'alloué, surveillance des volumes logiques, etc.),
- la surveillance « temps réel » des performances et des ressources des capacités et dispositifs (VM, serveurs, stockage, éléments réseaux, ...),
- le contrôle des seuils d'utilisation des capacités et dispositifs (serveurs, hyperviseurs, baies de stockage, réseaux, ...),
- la détection des coupures ou dégradations de service résultant du dépassement de ces seuils,
- le déclenchement des actions correctives (i.e. application de consigne, escalade notamment vers des personnes en astreinte hors horaire standard),
- la surveillance « temps réel » des alertes liées à la sécurité,
- le contrôle notamment des tentatives d'intrusion, des attaques virales, des tentatives d'effacement ou d'extraction de données.

#### → **Exploitation courante des dispositifs techniques :**

Le Titulaire assure :

- le traitement des incidents déclarés par le Pouvoir Adjudicateur,

- les travaux périodiques (transferts de fichiers, arrêt/relance des matériels, état des lieux, modification de droits, ...),
- le traitement des demandes standards,
- l'analyse de logs sur les couches techniques,
- la gestion de la sécurité des infrastructures (réseau, serveurs, tests périodiques d'intrusion périodiques, vérification des failles de sécurité, ...), et la production de rapports périodiques associés,
- l'analyse des historiques de fonctionnement « Logs »,
- l'analyse des comportements anormaux,
- la rédaction et le maintien à jour des documents opérationnels (consignes, procédures, check-lists, dossier d'exploitation, d'installation, gestion de la configuration...), via un outil de gestion documentaire,
- le pilotage de la maintenance matérielle et logicielle,
- la force de proposition sur le maintien en condition de sécurité,
- l'administration quotidienne des dispositifs techniques : socle virtualisation (switch virtuels, haute disponibilité, ...).

#### c. UO\_A4\_9 et UO\_A4\_9\_HDS : Sauvegarde des données

Cette UO permet de commander le backup complet ou partiel d'une VM ou d'un serveur physique.

#### d. UO\_A4\_10 : Service de PRA

Cette UO permet de mettre en place un service de PRA avec réplication multisite pour un serveur. Les serveurs sont à commander via les UO dédiées, la présente UO concernant la mise en place des services associés à la réplication des données et à la bascule d'un site à l'autre.

L'UO couvre la conception, la mise en œuvre, l'exploitation et la maintenance d'un service de PRA pour les infrastructures et applications critiques du pouvoir adjudicateur, garantissant une reprise d'activité rapide et sécurisée en cas de sinistre.

Le service inclut :

1. Architecture résiliente :
  - Réplication des données et des applications vers un site secondaire géographique distinct (distance minimale de 30 km) ;
  - Redondance des composants critiques (serveurs, stockage, réseau) avec une capacité équivalente à l'infrastructure principale.
2. Objectif de reprise inférieur ou égal à deux (2) heures, disponibilité cible de 99,95 % (hors maintenance programmée).
3. Sauvegardes automatisées, chiffrées et immutables, avec une rétention de trente (30) jours.
4. Bascule et tests :
  - Test complet de bascule (simulation de sinistre majeur) sur demande du pouvoir adjudicateur (avec l'UO\_A5\_4), avec un rapport détaillé transmis sous quinze (15) jours ;
  - Bascule automatique en cas de détection d'une panne majeure (ex : perte de connectivité, cyberattaque).
5. Documentation et support :
  - Procédures de PRA documentées et mises à jour annuellement ;
  - Support 24h/24 et 7j/7 pour la gestion des incidents et la bascule d'urgence.
6. Conformité aux normes ISO 22301 (continuité d'activité) et ISO 27001 (sécurité).

#### 4.9.4. Engagements et niveaux de service

Le Titulaire s'engage :

- à accepter des audits (réalisés par le Pouvoir Adjudicateur ou par un tiers) sur les infrastructures (stockage, réseau, virtualisation, ...) supportant les infrastructures mises à disposition du Pouvoir Adjudicateur (ex : contrôler que l'infrastructure virtuelle est bien conforme "à l'état de l'art", qu'elle est performante, contrôler que les ratios de consolidation sur l'infrastructure virtuelle sont inférieurs aux seuils préconisés, ...) sur demande du Pouvoir Adjudicateur conformément aux stipulations du CCAP ;

- à informer le Pouvoir Adjudicateur (avant la réalisation des opérations - 10 jours avant minimum) dès qu'il y a des mises à jour (patch sur les baies, montées de version sur la virtualisation, ...) sur les dispositifs techniques de l'infrastructure de l'Infrastructure virtuelle qui supporte le SI du Pouvoir Adjudicateur ;
- à disposer de générations de matériels (moins de 4 ans) et logiciels récentes (moins de 2 ans) à la mise en service ;
- à se conformer, sauf accord explicite contraire, aux bonnes pratiques en matière de gestion des sauvegardes : Stratégie dite « 3-2-1 », à savoir 3 copies des données dont 2 sauvegardées sur 2 types de supports différents et dont 1 des supports est physiquement hors site ; ce dernier doit, en outre, être déposé à une fréquence mensuelle dans les locaux de l'ANSM (voir ci-dessous) ;
- à se conformer, sauf accord explicite contraire, au schéma de rotation actuel de l'ANSM en matière de fréquence de sauvegarde et recyclage : Rotation apparentée au type « hiérarchie GFS » légèrement modifié comprenant une sauvegarde complète hebdomadaire (soit 52-53 sauvegardes par an) et 6 sauvegardes incrémentales journalières. La dernière sauvegarde hebdomadaire complète du mois devient la sauvegarde mensuelle (soit 12 sauvegardes mensuelles par an, à fournir à l'ANSM une semaine après son achèvement) ; le recyclage s'effectuera sur une période de quatre (4) semaines de façon à obtenir un RPO de vingt-huit (28) jours consécutifs puis douze (12) mois consécutifs ; la dernière sauvegarde mensuelle de l'année est conservée *ad vitam aeternam* sauf avis contraire (les 11 précédentes pourront être recyclées). Il faut donc prévoir sa relecture / restauration pendant plusieurs années (Engagement sur au moins la durée du contrat – même en cas de renouvellement).
- à fournir à l'ANSM tout moyen nécessaire à la relecture d'un jeu de sauvegarde mensuel si les dispositifs matériels et/ou logiciels standards ne suffisent pas.

Les classes de services des capacités fournies sont précisées au 4.6.2 du présent CCTP.  
Les engagements sont précisés dans la convention de services.

#### 4.9.5. Outillage de services

---

Le Titulaire doit disposer d'outils de surveillance pour la supervision, l'exploitation et l'administration des équipements (création / modification de VM, création / modification d'espace de stockage, récupération de sauvegarde, restauration de données..).

Cet outillage permet de produire les indicateurs de niveaux de services demandés conformément à la convention de services et les alertes.

Ces outils doivent être accessibles au Pouvoir Adjudicateur.

La mise à disposition de l'outillage de service ne fait pas l'objet d'un surcoût dédié. Le coût lié à la mise à disposition est compris dans les unités d'œuvres du module.

#### 4.9.6. Modèle Financier

---

Les prestations du module sont rémunérées conformément aux UO du BPU.

### 4.10. **Module A5 – Assistance technique, prestations complémentaires**

---

#### 4.10.1. Préambule

---

Ce module a pour but de définir les prestations d'expertises ponctuelles et d'urgence destinées à accompagner le Pouvoir Adjudicateur dans la mise en œuvre et le cycle d'exploitation des infrastructures techniques hébergées conformément au présent CCTP.

#### 4.10.2. Périmètre

---

L'ensemble des prestations demandées dans les modules A1 à A5 concernent des prestations standards Titulaire.

Toute demande non standard, et tous travaux liés à l'objet du marché en dehors des prestations incluses dans le périmètre des autres modules seront traités via le module A5 en mode projet (assistance technique).

A titre d'exemple, ce module peut être activé pour (liste non exhaustive) :

- Effectuer des tests de vulnérabilité de l'appliquet installé ;
- Proposer et mettre en place une solution technique d'hébergement d'une nouvelle plateforme sur spécifications fournies par le Pouvoir Adjudicateur.
- Effectuer une réversibilité sortante partielle, dans le cas par exemple d'une ré-internalisation de l'hébergement d'une application ou d'un service.

#### 4.10.3. Prestations attendues

---

Ces prestations « à la demande » confiées au Titulaire sont relatives à des opérations exceptionnelles.

##### a. UO\_A5\_1 à UO\_A5\_3 : Prestations d'assistance technique

---

Le Titulaire est responsable en pleine autonomie de la réalisation et du pilotage des prestations d'assistance technique jusqu'à sa phase d'exploitation.

La réalisation de ses prestations est pilotée par un chef de projet nommé par le Titulaire.

Le Titulaire est responsable de la production de la documentation associée.

Le Pouvoir Adjudicateur exprime son besoin et les objectifs spécifiques associés, à travers un cahier des charges qu'il transmet au Titulaire.

Les prestations attendues sont :

- fourniture sous un délai maximum de deux (2) semaines d'une proposition contenant :
  - La solution technique qu'il propose en réponse au besoin,
  - La méthodologie de conduite des prestations,
  - Les tâches à réaliser et les livrables associés,
  - Les échéances de réalisation des livrables,
  - La méthodologie de conduite du changement intégrant le plan de communication,
  - Sa proposition financière (avec les UO du BPU utilisées et la quantité),
  - Les profils proposés pour réaliser les prestations,
  - Le planning ;
- la réalisation des prestations :
  - la réalisation des tâches conformément à la proposition établie précédemment et reprise par/annexée au bon de commande ;
  - la transmission d'un bilan de prestations, précisant notamment les dates de réalisation des livrables et les éventuelles particularités survenues lors de la réalisation des prestations.
- le pilotage des prestations.

Le chiffrage de la proposition s'établit en fonction des profils suivants :

- Chef de projet,
- Technicien,
- Expert technique.

Le Pouvoir Adjudicateur est libre d'accepter ou de refuser la proposition du Titulaire en fonction de sa performance (risques, coûts, délais...).

Le lancement des prestations est effectif à la notification par le pouvoir Adjudicateur au Titulaire du bon de commande relatif aux prestations.

Le Titulaire exécute les prestations conformément aux dispositions prévues dans ledit bon de commande.

La recette sans réserve de ces prestations, conformément aux modalités précisées dans le présent document, valide l'atteinte de ces objectifs.

Les prestations d'assistance techniques sont réalisées dans les locaux du Titulaire.

##### b. Prestations complémentaires :

---

##### UO\_A5\_4 : Test de bascule PRA

---

Le Plan de Reprise d'Activité (PRA) constitue une composante essentielle de la stratégie de résilience du Titulaire. Dans une approche cloud-native, ce plan intègre systématiquement les principes suivants :

- Architecture multi-site : Réplication synchrone ou asynchrone des données et des services entre au moins deux (2) sites géographiquement distincts, garantissant une tolérance aux pannes et une reprise d'activité rapide en cas de sinistre majeur.
- Backups immutables : Les sauvegardes seront stockées dans un format immuable (WORM – Write Once, Read Many) et isolées des environnements de production pour se prémunir contre les suppressions ou corruptions malveillantes.
- Automatisation des procédures : Les processus de bascule et de restauration seront automatisés et documentés pour réduire les délais d'intervention et limiter les erreurs humaines.

Le Pouvoir Adjudicateur se réserve le droit de commander un test de bascule PRA à tout moment, selon une méthodologie convenue avec le Titulaire. Les résultats, incluant les métriques de performance (durée de bascule, perte de données, stabilité post-restauration) et les actions correctives identifiées, seront consignés dans un rapport détaillé transmis sous quinze (15) jours ouvrés. Ce rapport devra démontrer la conformité aux engagements contractuels et proposer, le cas échéant, un plan d'amélioration continue.

c. UO\_A5\_5 : Test de restauration des données

La restauration des données consiste à utiliser des sauvegardes pour remettre un système d'information qui a été altéré dans un état antérieur à l'altération.

Le Pouvoir Adjudicateur peut commander un test de restauration des données. Le résultat est le rapport de test.

d. UO\_A5\_6 : Test de montée en charge

La montée en charge consiste à qualifier l'architecture testée dans sa capacité à pouvoir supporter un nombre d'utilisateurs croissant sans défaillir.

Le Pouvoir Adjudicateur peut commander un test de montée en charge. Le résultat est le rapport de test.

e. UO\_A5\_7 : Test d'intrusion

Un test d'intrusion est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique.

La méthode consiste généralement à simuler une attaque d'un utilisateur mal intentionné, voire d'un logiciel malveillant, ou un Malware. Le testeur analyse alors les risques potentiels dus à une mauvaise configuration d'un système, d'un défaut de programmation ou encore d'une vulnérabilité liée à la solution testée.

Le Pouvoir Adjudicateur peut commander un test de montée en charge. Le résultat est le rapport de test.

f. UO\_A5\_8 : Audit de conformité HDS

Le Pouvoir Adjudicateur peut commander un audit de conformité HDS. Le résultat est le rapport d'audit qui indique les éventuelles défaillances aux exigences du cadre réglementaire.

g. UO\_A5\_9 : Audit de sécurité

L'audit peut être effectué dans différents buts :

- réagir à une attaque,
- se faire une bonne idée du niveau de sécurité du SI,
- tester la mise en place effective de la PSSI,
- tester un nouvel équipement,
- évaluer l'évolution de la sécurité (implique un audit périodique).

Dans tous les cas, il a pour but de vérifier la sécurité du dispositif en œuvre.

Le résultat est le rapport d'audit. Celui-ci contient la liste exhaustive des vulnérabilités recensées par l'auditeur sur le système analysé. Il contient également une liste de recommandations permettant de supprimer les vulnérabilités trouvées.



#### 4.10.4. Engagements et niveau de services

---

Il est demandé au Titulaire un engagement de résultat global, matérialisé par la production d'un livrable précis dans un délai défini et pour un coût fixé à l'avance.

Les objectifs assignés aux prestations d'assistance technique sont les suivants :

- Production de la proposition (solution, devis...) dans un délai de deux (2) semaines maximum,
- Respect du délai prévisionnel,
- Respect de la qualité des livrables (produit, documentation...),
- Respect du coût défini.

Les prestations d'assistance technique doivent être conduites sans altérer la qualité de service des opérations confiées au Titulaire et en toute indépendance du traitement de celles-ci.

Les niveaux de services et les engagements associés sont précisés dans la convention de services.

#### 4.10.5. Outillage

---

Le Titulaire fournit l'outillage permettant au Pouvoir Adjudicateur d'effectuer sa demande, d'en suivre évolution et de valider la bonne réalisation.

La mise à disposition de l'outillage de service ne fait pas l'objet d'un surcoût dédié. Le coût lié à la mise à disposition est compris dans les unités d'œuvres du module.

#### 4.10.6. Modèle Financier

---

Les prestations du module sont rémunérées conformément aux UO du BPU. Par exception, les frais liés à un audit conduit ou mené par ou à la demande du Pouvoir Adjudicateur pourront être mis à la charge du Titulaire et dans les conditions et les cas limitativement énumérés au CCAP.

### 4.11. Module A6 – Pilotage et Accompagnement

---

#### 4.11.1. Principes généraux

---

##### a. Interlocuteur

---

Le Titulaire désigne nommément un interlocuteur unique pour ce marché. De son côté, le Pouvoir Adjudicateur désigne également un interlocuteur unique pour ce marché. Il est destinataire de l'ensemble des incidents signalés et de leur résolution.

##### b. Transparence

---

Le Pouvoir Adjudicateur doit conserver en permanence la connaissance du niveau de la qualité du service rendu et par ailleurs les moyens de vérifier que les engagements contractuels sont tenus.

Ainsi, l'activité du Titulaire est « tracée » et donne lieu à la production de tableaux de bord périodiques contenant des indicateurs de cette activité. Ces tableaux de bord doivent être documentés par le titulaire.

##### c. Capacité à être audité

---

Le Pouvoir Adjudicateur se réserve également la possibilité de faire auditer tout ou partie de la prestation de service pour vérifier que le Titulaire satisfait à ses obligations et aux exigences de qualité de service de la Convention de Service.

Les audits peuvent porter sur tous les domaines.

Le Titulaire s'engage à respecter l'obligation de mise en conformité qui serait prononcée par ces audits.

##### d. Evolutivité du service

---

Le service est réputé évolutif lorsque son organisation sait s'adapter à des changements portant sur le volume de sollicitations (accroissement ou réduction) ou à une modification de leur nature tout en restant conforme au périmètre du marché.

Les types majeurs d'évolutions à considérer sont :



- Les évolutions significatives de volumétrie à la hausse comme à la baisse, par exemple lors de l'intégration d'une nouvelle application ou d'un nouveau service ;
- Les évolutions de périmètre technique, par exemple lors de l'apparition d'une nouvelle technologie.

#### e. Relation partenariale

Le Pouvoir Adjudicateur attend du Titulaire un rôle de conseil et un comportement proactif pour notamment :

- prévoir les dysfonctionnements, en particulier par l'analyse des tendances des incidents récurrents, et en avertir le Pouvoir Adjudicateur par anticipation,
- apporter un conseil au Pouvoir Adjudicateur lorsqu'il prend des décisions qui s'imposent aux équipes du Titulaire, et sont susceptibles de modifier la qualité de service fourni,
- Apporter un conseil au Pouvoir Adjudicateur au niveau du maintien de condition de sécurité sur le SI hébergé.

Le Pouvoir Adjudicateur entend rappeler que, dans le cadre du présent marché, il est déterminant que le Titulaire :

- collabore de manière effective et spontanée avec tous les tiers contractuellement liés au Pouvoir Adjudicateur et pouvant avoir un lien avec l'exécution du marché ;
- soit particulièrement réactif en cas de problème, quel qu'il soit, lié à l'exécution du service :
  - en communiquant au plus tôt au Pouvoir Adjudicateur l'existence dudit problème dès qu'il en a connaissance,
  - en collaborant de manière active à sa résolution dans la mesure de ses moyens, même si l'incident est hors de son périmètre de responsabilité.

#### f. Production des tableaux de bord

Les informations permettant de mesurer les indicateurs de qualité de service sont définies conjointement par le Pouvoir Adjudicateur et le Titulaire lors de la phase de prise en charge.

Le Titulaire assure la production et la mise à jour de tableaux de bord pour chaque fonction assurée, et selon le format et le niveau d'information requis par le Pouvoir Adjudicateur.

La fréquence de production de ces tableaux de bord est trimestrielle au début du marché. Elle est revue en cours de marché, au fur et à mesure de l'évolution du périmètre du marché sans pour autant être réduite en deçà du mois.

Les tableaux de bord sont analysés lors des comités de pilotage et/ou des comités techniques auxquels participe le responsable de la prestation.

#### g. Conseil et état de l'art

Le Titulaire a une obligation de conseil continu auprès du Pouvoir Adjudicateur afin de contribuer à l'amélioration de la performance des prestations qui lui sont confiées et à la réduction des coûts des services associés.

L'apport de conseil porte notamment sur :

- les technologies : tendances, opportunités, caractéristiques, valeur ajoutée, ...
- les nouvelles versions et/ou les versions en place qui ne sont ou ne seront plus supportées,
- l'amélioration de l'organisation et de la coordination,
- les opportunités de réduction de coûts,
- les opportunités d'amélioration de la qualité des services,
- la sécurité,
- la gestion des risques.

Il est attendu du Titulaire d'avoir un apport important sur ces champs compte tenu de son expérience et de sa visibilité des contrats et de ses capacités de mutualisation des moyens de veille et de tests.

#### 4.11.2. Exigences de qualité dans la réalisation du service

---

##### a. Mise en place de processus de qualité de service

---

Les différentes prestations du marché doivent s'accompagner de la mise en œuvre de meilleures pratiques de production des services informatiques en s'appuyant sur les processus (ITIL).

##### b. Réversibilité du service

---

Le Titulaire sortant s'engage à assurer la réversibilité du service afin de permettre au Pouvoir Adjudicateur de reprendre ou de faire reprendre par un tiers la fourniture du service et ce, dans les meilleures conditions.

Les dispositifs assurant la complète opérationnalité de la réversibilité sont consignés par le Titulaire dans le plan de réversibilité et dans les PAQ et PAS lors de la prise en charge, puis mis à jour tout au long du marché.

Il décrit notamment la maîtrise de la gestion des biens (inventaire, configuration, ...), de la gestion documentaire (processus, procédures, consignes, ...), des procédures et outils de contrôle opérationnel, et des procédures liées aux prestations de support associées.

Le plan de réversibilité doit pouvoir être appliqué partiellement par service, par modules. Il inclut et précise ses modalités de participation et d'aide active de transmission (processus de transmission, données, documents et informations transmis).

Une fois commandée, la réversibilité est mise en œuvre en parallèle de la fin de la Phase de Service Régulier.

Le Titulaire est tenu à un devoir d'information auprès du Pouvoir Adjudicateur concernant tous les éléments spécifiques (matériels, logiciels, organisations, ...), par rapport aux standards constatés sur le marché, qui pourraient représenter une difficulté au cours de la mise en œuvre de la réversibilité.

##### c. Documentation et capitalisation

---

Le Titulaire conçoit, si elle n'existe pas, et maintient une documentation opérationnelle exhaustive de tous les services (ensemble des activités donnant lieu à la facturation d'une UO) sous sa prestation, et mettra à la disposition du Pouvoir Adjudicateur une version complète à jour à minima tous les ans, lors des revues du plan de réversibilité, et sous un délai d'un (1) mois à la demande du Pouvoir Adjudicateur. La liste de ces documentations est proposée par le Titulaire lors de la phase de prise en charge, et soumise à validation du Pouvoir Adjudicateur.

Toute nouvelle version de document annule et remplace la précédente. Il est de la responsabilité du Titulaire de détenir et d'appliquer la dernière version validée.

En particulier, le Titulaire a la charge de les communiquer et de les expliquer aux intervenants de ses équipes et à ses éventuels sous-traitants.

##### d. Maîtrise de la prestation et de la qualité de service

---

Le Titulaire est responsable des prestations décrites aux chapitres précédents. A ce titre, il lui incombe de se doter des méthodes, outils et organisation, dans le respect des contraintes liés au contexte du Pouvoir Adjudicateur, qui lui permettent :

- d'exécuter ses prestations avec le niveau de qualité et de sécurité requis,
- d'en surveiller la constance,
- de prendre les dispositions de maintien ou d'améliorations qui s'imposent,
- d'apporter au Pouvoir Adjudicateur transparence et justification sur ce qui est fait.

Le Titulaire dispose d'un système qualité et sécurité exposé dans un ensemble de dossiers et documents associés approuvables par le Pouvoir Adjudicateur.

Ces documents sont fournis et/ou mis à jour à l'occasion de chacune des phases de prise en charge. Ils sont mis à jour pendant toute la durée de la prestation d'hébergement.

Le Titulaire s'engage à fournir au Pouvoir Adjudicateur l'ensemble des dossiers de son système qualité sur simple demande, et à faire appliquer les recommandations par son équipe et par ses éventuels sous-traitants.

Ces documents doivent constituer un cadre de référence cohérent utilisable par tous les participants et intervenants du présent marché. Il doit faire apparaître clairement les liens entre les services, les activités, les responsabilités, les tâches et les produits. La planification doit permettre d'anticiper et prévenir les dérives et les risques. Le Pouvoir Adjudicateur précise que le Titulaire doit prendre en compte les délais de validation et d'approbation des produits livrés.

#### 4.11.3. Dispositif de pilotage du marché et Prestations attendues

Le pilotage de la prestation par le Titulaire regroupe les activités liées aux réunions de pilotage et de contrôle, les activités de maîtrise de la prestation et de la qualité de service et les activités de sécurité. Les réunions de pilotage sont les Comités de Pilotage, le Comité de Suivi et le Comité de Sécurité.

Leurs décisions ne peuvent modifier le marché public.

Sa mission principale est la coordination de l'ensemble des prestations fournies et le contrôle de la qualité de service.

##### a. UO\_A6\_1 : Gestionnaire opérationnel de compte

Le Pouvoir Adjudicateur peut commander une UO « gestionnaire opérationnel de compte ».

Ce gestionnaire :

- anime le Comité de Pilotage,
- prend en charge la responsabilité commerciale et économique du marché,
- est garant du respect des engagements et de la qualité de service,
- est en mesure d'engager le Titulaire,
- assure la coordination de l'ensemble des prestations pour le Pouvoir Adjudicateur,
- veille à la qualité opérationnelle du service,
- met en œuvre les moyens, garantit leur permanence, les adapte afin de respecter les engagements contractuels,
- propose des plans d'amélioration ou d'actions correctives.

Le Pouvoir Adjudicateur désigne de son côté, pour le suivi de l'exécution des prestations, un responsable du marché qui s'assure de la bonne exécution des prestations.

Le responsable du Titulaire et le responsable du marché du Pouvoir Adjudicateur ont autorité suffisante chacun pour prendre ensemble toutes décisions opérationnelles courantes communes.

Le Titulaire peut proposer d'autres modalités d'échange afin de répondre aux exigences de qualité et d'optimisation et rationalisation de la qualité de service qui guident la prestation.

Le dispositif de pilotage est à préciser par le Titulaire dans son « Plan Assurance Qualité ».

##### b. Comité de Pilotage

Le Comité de pilotage, notamment :

- Contrôle la qualité des Prestations exécutées par le Titulaire,
- Décide de plans d'améliorations,
- Suit l'avancement des projets,
- Préconise des évolutions de périmètre et des services,
- Prépare les orientations et les évolutions du système informatique.

Le Comité de Pilotage est composé de représentants du Pouvoir Adjudicateur et du Titulaire.

La fréquence de ces comités de pilotage sera mensuelle pour les trois (3) premiers mois de la prestation. Elle sera ensuite trimestrielle.

C'est au cours de ce comité que le Titulaire présente une synthèse des événements de la période écoulée, tant sur le plan qualitatif que quantitatif, et des prévisions pour la période suivante. Au cours de cette réunion, les parties échangent sur le niveau de qualité de service atteint et éventuellement sur les pénalités applicables en s'appuyant notamment sur les éléments suivants :

- Une analyse du service rendu, qu'il s'agisse du service ou des prestations associées,
- Des indicateurs de suivi de l'activité de support,
- Un bilan détaillé sur les incidents de la période,

- Un planning détaillé des activités du mois suivant,
- Un planning macroscopique pour les activités à moyen terme,
- Un état des carences et des non-conformités de service,
- Un état de la gestion des actions en matière de qualité et de sécurité,
- Un état du suivi des livrables,
- Un état du suivi des Prestations d'appropriation/réversibilité,
- Un état du périmètre infogéré,
- Un état du volume d'activité par prestation,
- Un point sur la gestion de la réversibilité,
- Un état sur les ressources consommées et les bons de commandes dans le cadre des prestations en obligation de moyens renforcée,
- Les événements contractuels et administratifs (facturation, dérogations, réclamations, avenants).

Le Comité de Pilotage peut demander la participation de tout intervenant nécessaire, compte tenu de l'ordre du jour, l'autre partie pouvant s'y opposer pour des raisons de confidentialité.

Le secrétariat du comité (ordre du jour, compte rendu) est assuré par un représentant du Titulaire.

Le compte rendu de chaque réunion du Comité de Pilotage est approuvé par les représentants des deux (2) parties dans un délai de cinq (5) jours à compter de l'émission du compte rendu.

En cas de points de vue opposés et non conciliables, le différend est acté dans le compte rendu.

D'autres instances de coordination et d'optimisation du service pourront être prévues dans le PAQ, en particulier un Comité de Pilotage exceptionnel peut avoir lieu pour la gestion de crise (estimé à un par mois au maximum).

#### c. UO\_A6\_2 : Gestionnaire applicatif

Le Pouvoir Adjudicateur peut commander une UO « gestionnaire applicatif ».

Ce gestionnaire :

- anime le Comité de Suivi,
- prend en charge la responsabilité technique d'une application,
- prend en charge les demandes de travaux,
- est garant du respect des engagements et de la qualité de service.

#### d. Comité de Suivi

Le Comité de Suivi prend en charge la réalisation des actions de mise en place, s'assure de l'affectation et de la disponibilité des ressources et mesure les impacts de toute évolution de service.

Le Comité de Suivi se réunit en fonction du besoin (avec un maximum d'un comité de suivi par mois) et est composé de représentants du Pouvoir Adjudicateur et du Titulaire ayant des responsabilités techniques dans le cadre du présent marché.

C'est au cours de ce comité que le Titulaire vérifie la disponibilité des ressources humaines et techniques, identifie les risques de perturbations et présente une synthèse des événements marquants relatifs aux activités du Titulaire de la période écoulée en s'appuyant a minima sur les éléments suivants :

- Un bilan détaillé sur les incidents de la période,
- L'identification des difficultés rencontrées ou potentielles,
- Des indicateurs de suivi de l'activité de support,
- Le suivi des actions d'amélioration des services,
- Le suivi des actions de sécurité, des incidents de sécurité et du maintien en condition de sécurité,
- La planification des tâches des semaines à venir,
- Le suivi et la programmation des demandes de travaux (bilan des déploiements matériels, état des demandes de travaux et planning prévisionnel, identification des difficultés rencontrées ou potentielles, ...).

#### e. UO\_A6\_3 : Responsable Sécurité

Le pouvoir adjudicateur peut commander une UO « Responsable Sécurité ».

Ce responsable :

- anime le Comité de Sécurité tel que décrit à l'article 4.3.6 « Règles de Sécurité » du présent CCTP,
- prend en charge la responsabilité de la sécurité,
- suit l'avancement du plan d'actions sécurité, le traitement des incidents de sécurité, l'avancement des travaux de couverture ou réduction des risques,
- établit un bilan des alertes remontées et des correctifs de sécurité installés, le suivi des résultats des audits menés et des plans d'actions associés.

#### 4.11.4. Modèle Financier

---

Les prestations du module sont rémunérées conformément aux UO du BPU.

#### ▪ Liste récapitulative des annexes au présent CCTP :

Nature	Dénomination
Fiche d'architecture technique	Annexe 1 - Hébergement - Fiche architecture technique
Convention de services	Annexe 2 - Hébergement - Convention de services