



CCTP – Infogérance des infrastructures informatiques et prestations associées.

VERSION 2.1

I. Table des matières

I.	Table des matières.....	1
II.	Grille de lecture.....	2
III.	Objet & périmètre.....	2
a.	Contexte et objet du marché.....	2
b.	Présentation de l'Anah.....	3
c.	Autres acteurs.....	3
d.	Les grandes phases du marché.....	3
e.	Le contexte technique.....	4
1.	Hébergeur actuel et volumétrie.....	4
2.	Architecture générale.....	5
3.	Liste des applications.....	5
4.	Composants managés.....	8
5.	Périmètre en obsolescence.....	8
6.	Indicateurs de performance.....	9
f.	Les exclusions de périmètre.....	9
IV.	Exigences transversales.....	10
V.	Modèle de gouvernance.....	16
a.	Exigences communes à toutes les phases.....	16
b.	Exigences pendant les phases de réversibilité.....	20
c.	Exigences pendant la phase de RUN nominale (post-réversibilité entrante).....	23
VI.	Prestations attendues pendant les phases de réversibilités.....	27
a.	Exigences au titre de la réversibilité entrante.....	29
b.	Exigences au titre de la réversibilité sortante.....	36
VII.	Catalogue de principaux services.....	38
a.	Gestion des demandes.....	39
b.	Gestion des incidents.....	43
c.	Gestion des problèmes.....	45
d.	Gestion des changements.....	47
e.	Gestion des configurations.....	50
f.	Gestion des déploiements.....	51
g.	Gestion de la continuité de service.....	56
h.	Gestion des sauvegardes.....	58
i.	Supervision et monitoring.....	60

II. Grille de lecture

Le présent document décrit sous forme d'exigences les attentes de l'Anah vis-à-vis du TITULAIRE.

L'offre du titulaire précise et argumente les propositions en réponse aux exigences décrites dans le présent CCTP.

Chaque exigence est présentée selon le formalisme suivant :

Identifiant unique de l'exigence : Intitulé court de l'exigence
Une description la plus claire possible de l'exigence.
<i>Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :</i> Description du niveau à atteindre / ce qui est contrôlé

Toutes les prestations seront exécutées sur la base de bons de commande émis par l'Anah. Certaines de ces prestations, bien que déclenchées par bons de commande, auront un caractère récurrent (par exemple des interventions régulières ou des prestations réitérées dans le temps).

Par ailleurs, certaines exigences seront traitées sous forme de prestations au forfait, associées à une unité d'œuvre ou à un périmètre bien défini. Pour ces prestations forfaitaires, le soumissionnaire s'engage sur un résultat, un livrable ou un niveau de service précis, pour un prix global fixé à l'avance, tel que décrit dans le bordereau de prix. Ainsi, le bon de commande viendra simplement activer la réalisation de ces prestations, qu'elles soient unitaires ou forfaitaires, en précisant les unités d'œuvre concernées et leur périmètre d'intervention.

III. Objet & périmètre

a. Contexte et objet du marché

L'Agence nationale de l'habitat ci-après l'Anah poursuit la modernisation et la sécurisation de son infrastructure informatique. Celle-ci se place dans un environnement réglementé et embarque des actifs critiques pour le bon fonctionnement de l'établissement.

L'objectif du présent marché est de confier à un TITULAIRE unique l'infogérance complète de l'infrastructure informatique de l'Anah, afin d'en assurer la disponibilité, la performance, la sécurité et l'évolutivité. À ce titre, le TITULAIRE est chargé d'exploiter, de maintenir et de superviser l'ensemble des ressources IT (matériels, logiciels, réseaux, systèmes et services associés), dans le respect des niveaux de service définis au marché, tout en accompagnant l'Anah dans l'optimisation et la modernisation de son système d'information. Dans ce contexte, le TITULAIRE est un professionnel expérimenté dans l'infogérance de bout en bout des infrastructures IT OnPremise et sur le Cloud.

Le TITULAIRE a une obligation de conseil vis-à-vis de l'Anah. Ces conseils peuvent être d'ordre technique (choix d'un matériel, choix d'une instance, choix d'une configuration) et/ou pratique (risques, prise de recul, retour d'expérience ...) cela dans le cadre du bon fonctionnement de la plateforme IT de l'Anah.

À la date de la consultation, le Système d'Information de l'Anah est en partie externalisé dans le cadre d'un contrat qui arrive à échéance le 18 mai 2027. Ce contrat a pour périmètre l'hébergement et les services de gestion qui y sont associés.

Les pénalités applicables, les modalités de paiement, les avances, la sous-traitance, la résiliation et les assurances sont régies par le CCAP.

b. Présentation de l'Anah

L'Agence nationale de l'habitat est un établissement public administratif de l'État placé sous la tutelle du ministère chargé du logement et du ministère chargé des finances. Créée en 1971, elle a pour mission de mettre en œuvre la politique nationale de développement et d'amélioration du parc de logements privés existants. Pour atteindre cet objectif, elle encourage l'exécution de travaux en accordant des subventions aux propriétaires occupants, aux propriétaires bailleurs de logements locatifs et aux copropriétaires. Sa vocation sociale l'amène à se concentrer sur les publics les plus modestes.

L'Anah encourage et facilite ainsi l'exécution de travaux de réparation, d'assainissement, d'amélioration et d'adaptation d'immeubles d'habitation, ainsi que l'exécution de travaux de transformation en logements de locaux non affectés à l'habitation, dès lors que ces logements sont utilisés à titre de résidence principale.

Les travaux dans l'habitat privé existant soutenus par l'Anah s'inscrivent dans les grandes politiques nationales de traitement pérenne des enjeux de sécurité, de salubrité, d'accessibilité, d'adaptation au handicap, d'économie d'énergie et, de façon générale, de prise en compte du développement durable.

Pour assurer ses missions, l'Anah dispose de moyens techniques pour l'instruction des dossiers (applications métiers OP@I, Cronos, ROD, référentiel d'orientation des demandeurs et Contrats Anah en particulier pour le réseau métier, et les sites monprojet.anah.gouv.fr, maprimerenov.gouv.fr, le registre national des copropriétés, ouverts plus largement au public ainsi que des sites internet pour la communication interne ou externe (anah.fr, site public d'information de l'Anah, extranah.fr, site extranet de l'Anah) ou d'autres applications (Clavis, SSO de l'Anah). Un complément d'information sur ces applications est fourni en annexe.

c. Autres acteurs

Outre le TITULAIRE du présent contrat et l'Anah, dont l'acteur principal est la DSIN (Direction des Systèmes d'Information Numérique) d'autres acteurs sont parties prenantes :

- Hébergeur actuel : Le titulaire du contrat d'hébergement au moment du lancement de la consultation devant aboutir à la conclusion du présent contrat.
- Tierce-maintenance : Prestataires désignés, titulaires des contrats de maintenance des applications ou sites internet de l'Anah hébergés sur le site externalisé de l'hébergeur

Ponctuellement d'autres acteurs de certification et étatiques peuvent être amenés à intervenir sur le présent marché tels que (liste non exhaustive) :

- Autorités de certification : ANSSI, CNIL ...
- Auditeurs tiers indépendant : ISO 27001...
- Ministère de tutelle

d. Les grandes phases du marché

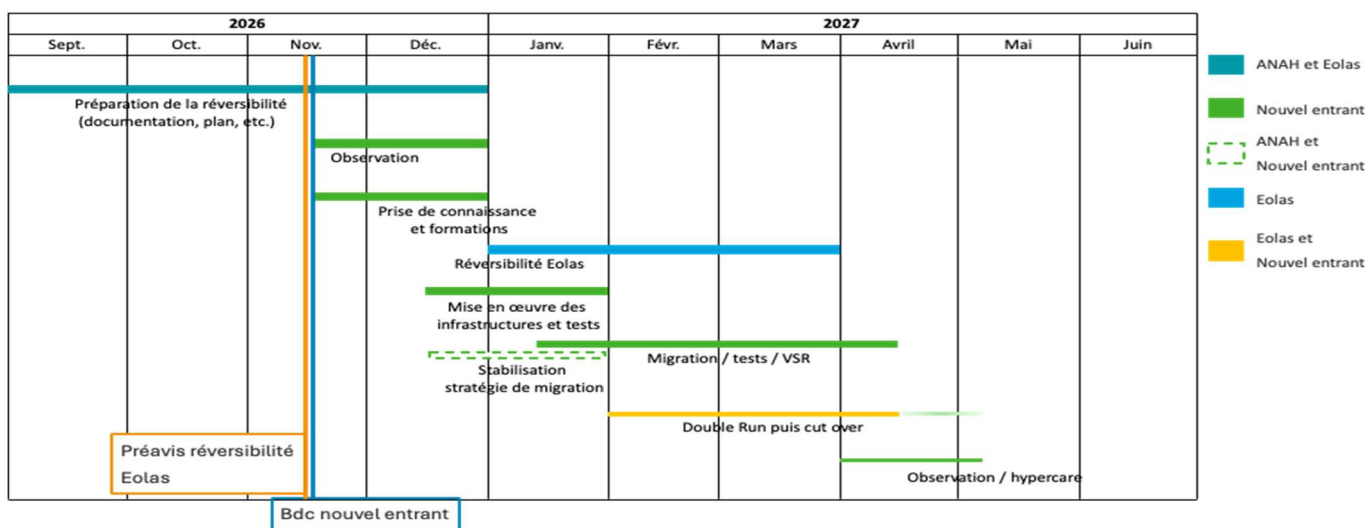
Dans le cadre de la mise en place du marché, quatre grandes phases sont identifiées et seront décrites plus exhaustivement dans les exigences. Ces phases sont associées à la réversibilité entrante en début de contrat et à la réversibilité sortante en fin de contrat.

Phases	Description et activités
Phase 1	- Notification du marché et prise de connaissance complète du périmètre. - Mise en place du dispositif humain et technique de la reprise - Prise de contact avec l'infogérant sortant et récupération de la documentation
Phase 2	- Migration des assets vers le nouvel hébergement - Reprise en exploitation (reverse shadow imbriqué) - Fin de migration et fin de reverse shadow

Phase 3	- Exploitation nominale de l'infrastructure IT - Mise en place et exécution des instances de gouvernance - Amélioration continue (Rebuild, Conteneurisation, FinOps, Gestion d'obsolescence)
Phase 4 – Réversibilité sortante	- Prise en contact avec l'exploitant entrant en phase de renouvellement de marché - Mise en place de l'exploitation (shadow) et fourniture de la documentation - Accompagnement, formation et transfert vers le nouveau TITULAIRE - Exploitation en reverse shadow - Fin de l'exploitation et transfert complet vers le nouveau TITULAIRE

Le détail de ces phases est décrit dans le chapitre V.

Le planning de réversibilité entrante envisagé est le suivant :



e. Le contexte technique

Le présent marché s'inscrit dans un environnement technique existant dont les principales caractéristiques sont décrites ci-après. Le TITULAIRE doit en prendre connaissance et en tenir compte dans l'exécution de ses prestations.

1. Hébergeur actuel et volumétrie

À la date de la consultation, le SI de l'Anah repose sur une architecture hybride, combinant :

- Des **ressources hébergées on-premise par l'Anah sur le site Opéra (Paris)**,
- Et des **ressources hébergées (sur une infrastructure VMware) et infogérées par le titulaire sortant, identifié comme EOLAS (OBS)**.

Cette organisation est héritée et s'est construite de manière progressive, dans un contexte de forte montée en charge de l'activité de l'Anah ces dernières années. À la date de rédaction du présent CCTP, le SI représente un périmètre d'environ 20 applications.

Les éléments ci-dessous sont communiqués à titre indicatif et peuvent évoluer au cours de l'exécution du marché.

Hébergement	Nombre de VM	vCPU	RAM totale (Go)	Stockage total (To)
Eolas	336	3567	12524	121
Opéra	91	273	819	24
Total	427	3840	13343	145

Les ressources sont réparties entre environnements de production, préproduction, et de développement. Le TITULAIRE doit tenir compte de cette volumétrie initiale, ainsi que de son évolution potentielle, afin de garantir la capacité, la performance, la résilience et la réversibilité attendues dans le cadre du marché.

2. Architecture générale

À la date de la consultation, le SI de l'Anah s'appuie sur une architecture majoritairement virtualisée. Les applications critiques, notamment celles exposées au grand public, sont hébergées par Eolas. Des composants logistiques et certains actifs internes sont hébergés sur le site d'Opéra.

L'architecture repose essentiellement sur des machines virtuelles, avec une gestion des environnements techniques partagée entre l'Anah et l'hébergeur selon les périmètres (OS, middleware, bases de données).

L'environnement ne dispose pas à ce stade de mécanismes natifs d'élasticité ou d'auto-scaling, et la scalabilité repose principalement sur des ajustements manuels de capacité. Une ambition initiale de recours à la conteneurisation orchestrée a été identifiée, notamment via Kubernetes.

Une part significative des applications historiques demeure structurée selon des architectures monolithiques ou n-tiers, généralement organisées autour d'un front applicatif et d'une base de données. Parallèlement, une évolution progressive vers des architectures orientées services est observée : environ 80 % des applications récentes ou transformées reposent sur des approches de type micro-services, majoritairement implémentées sous forme de conteneurs unitaires « mono-containers » encapsulant l'ensemble des composants applicatifs nécessaires à leur fonctionnement.

Les échanges entre applications internes et partenaires externes s'appuient sur des mécanismes d'interconnexion sécurisés et maîtrisés, incluant des API, des flux batch, des transferts de fichiers sécurisés et des web services. Les échanges inter-applicatifs sont strictement encadrés et reposent sur des modes standardisés tels que les API REST/JSON, la messagerie asynchrone de type Kafka et les transferts de fichiers via SFTP. Une préférence est accordée aux architectures asynchrones afin de favoriser le découplage applicatif, la résilience et l'évolutivité des échanges.

3. Liste des applications

À la date de la consultation, la liste des services intégrés dans le SI de l'Anah est décrite ci-après. Cette liste constitue le périmètre initial des éléments couverts par le projet et peut être enrichie et ajustée en fonction des nouveaux besoins exprimés par l'Anah tout au long de la période d'infogérance. Elle a vocation à évoluer afin de refléter au mieux les transformations du système d'information, les priorités métier et les exigences opérationnelles.

Chaque service recensé s'inscrit dans une logique de continuité de service et de maintien en conditions opérationnelles, avec une attention particulière portée à la qualité de service, à la performance et à la sécurité.

Application	Description
Domaine 1	
SEL - Service en ligne	Front Office de dépôt d'une demande de subvention d'aide à la pierre. Back Office de validation de la complétude d'un dossier.
France Renov	Plateforme pour informer, guider et orienter les ménages souhaitant réaliser des travaux de rénovation énergétique de leur logement (avec services numériques proposés) - Service public

France Renov - V2	Portail numérique de référence et guichet unique dédié à la rénovation de l'habitat privé, offrant un parcours utilisateur fluide de l'information à l'octroi des aides, grâce à un espace personnalisé nominatif, un accompagnement et une démarche proactive de conseil et d'orientation avec redirection vers les portails compétents pour la création de comptes et la gestion des dossiers des différentes aides (MPR ou SEL).
Anah.gouv.fr	Site institutionnel de l'Anah
AidesRénov	Simulateur des aides
Registre des copropriétés (RNC)	Registre National des Copropriétés (toutes infos sur les copropriétés) Immatriculation des copropriétés Restitutions statistiques destinées aux services des collectivités territoriales et à l'état Diffusion des statistiques et des recherches dans l'annuaire des copropriétés pour le grand public
Domaine 2	
Opal & Cronos	Opal : Back Office pour Mon Projet Anah (MPA), anciennement aides déléguées à la pierre. C'est un outil d'instruction (engagement/calcul/paiement) des dossiers d'aide de l'Anah Cronos : Outil d'instruction des dossiers soldés, de signalement et de fraude. Sert également de base d'archive
MPR FO (pega) [rattaché au Domaine 1]	Front End de Ma Prime Renov, application web permettant la gestion de l'attribution de prime dans le cadre de rénovations énergétiques d'un habitat.
MPR BO (pega) & Maileva	MPR BO : Backoffice de gestion des demandes de subvention Ma Prime Renov pour l'administration permettant l'instruction et la gestion des dossiers. Maileva : outil de gestion des courriers
Domaine 4	
ROD	Référentiel d'Orientation des Demandeurs (ROD), a pour vocation d'orienter dynamiquement les demandeurs de subvention Anah, en fonction de l'adresse de leur logement à rénover et la ou les thématique(s) vers les intervenants concernés (Pris, opérateurs...)
SI Agrément MAR ("Plateforme AMAR")	Le SI d'Agrément ouvre en Avril 2023 (AMAR). Il doit permettre le dépôt, l'instruction et l'octroi d'une demande d'agrément afin qu'un Accompagnateur Rénov' soit officiellement agréé et référencé. L'agrément est valable pour une durée de 5 ans renouvelable (le renouvellement de l'agrément se réalise par décision expresse de l'Anah)
Contrat Anah	Contrats Anah est une application qui permet une vision consolidée des engagements financiers de l'Anah et des objectifs prévus dans les conventions de programmes.
ExtraRénov	Nouvelle version de l'Extranet de l'Anah : Extra Renov)
Conseil Renov (ODC)	SareRenov
BDD Renov (ODC)	L'outil BDD Rénov' est le référentiel de données des outils SARE (SARénov', TBS, Calculindic) permettant à certains utilisateurs (selon les droits associés à leur profil) d'administrer les informations de l'ensemble des structures et des comptes utilisateurs de leur territoire.
Domaine 5	
RT	Outil de ticketing interne Request Tracker de Easter Eggs
Y2, Cegid - Patrimoine	Outil de gestion comptable et financière. Enregistrement du budget, des engagements. Achats d'actifs
Ligis	Outil de gestion des litiges Traitement juridique et comptable

Tempo	Tempo (Incovar+) est le logiciel de Gestion du temps de travail développé par la société Incotec. Le service RH apporte aux utilisateurs l'assistance de 1 ^{er} niveau et 2 ^e niveau (pour le 2 ^e niveau en lien avec le support technique d'Incotec). Pour le 3 ^e niveau en lien avec la DSIID et le support technique d'Incotec (nécessite connexion Teamviewer ouverte par DSIID).
Win-paie	Logiciel de gestion de la paie. Un fichier est envoyé à la DGFIP pour traitement.
Anahform (Talentsoft)	AnahForm est la solution Formation de TalentSoft. Cette plateforme est collaborative, et en conformité réglementaire RGPD. Les administrateurs, côté Formation apportent aux utilisateurs (agents siège + réseau) un niveau de réponse de base. Un niveau plus fin est assuré par un système de ticketing chez TalentSoft ou par le support technique du prestataire BearingPoint.
Jira / Confluence	Espace documentaire (Projets, Ticket, ...)
TalkSpirit	Outil collaboratif fournissant des espaces et des canaux de communication (Tchat, Vidéo Conf,...)
Eulerian	Outil de suivi des audiences web
Mailjet	Outil de mailing fourni par un prestataire, partagé par plusieurs applicatifs
Virtualia	Gestion de la paie, entretien professionnel, portail agent, gestion des temps
DATA	
Outils de connaissance du parc privé	Outil de gestion du parc privé : https://outils-parc-prive.anah.fr/ Outil de connaissance du parc privé au même titre que le RNC
MDM	Outil de Master Data Management (MDM), Application permettant de gérer le stockage & la qualité des données de référence du SI. Hébergée chez Titulaire sortant. En production mais non utilisé à date - Seules données des données géographiques (communes, région, ...)
ArcGIS	Outil pour créer des cartes (ou carte + édito) pour un accès grand public ou interne. Application en SaaS en prod mais pas utilisée par l'Anah ni le grand public
ETL	Outil de chargement (ETL) pour l'infocentre (Traité dans l'infocentre)
Infocentre	Entrepôt de données en interne pour les données référentielles de tous les applicatifs qui ne sont pas administrés comme des référentiels, y compris ETL Hébergée en interne Anah.
Datafabrik	Infocentre très large (Datalake, DW, ETL, ...). Pas encore mis en place (mais mise en production proche)
Power BI	Outil de Reporting pour France Renov et MPR. Reprise ADEME en cours (à traiter ultérieurement)
TBS	Tableau de bord des indicateurs du programme SARE. Reprise ADEME en cours (à traiter ultérieurement)
CalcullIndics	Outil de production d'indicateurs à partir des données de SARenov. Alimente TBS. Reprise ADEME en cours (à traiter ultérieurement)
Data Fabrik	Infocentre très large (Datalake, DW, ETL, ...). Pas encore mis en place (mais mise en production proche)
SAP - BO	Outil de reporting pour les experts métiers DAFC et RNC en consultation. Reprise ADEME (à traiter ultérieurement)
Anah (SIDP) & Socle Technique	
Authentification Externe (SSO externe)	Permet l'authentification des usagers dans le produit MPR : - Via France Connect - Login / Mot de passe

Clavis 1	Système de gestion des services et comptes web des internes. LemonLDAP. Hébergé chez Titulaire sortant.
Clavis 2	WEBSSO interne, Authentification interne. Au travers du jeton SSO, fournit les habilitations et droits d'accès pour OPAL. Hébergé chez OVH (Linagora).
Référentiels	Administration facilitée et centralisée des comptes Etablissement d'un référentiel unique découplé de l'identité Passage des applications à une authentification unique (SSO)
Dynatrace	Plateforme de supervision applicative et d'observabilité qui permet de détecter automatiquement les incidents, d'analyser les causes racines et de garantir la performance, la disponibilité et la sécurité des applications et infrastructures.
Forge	Usine logiciels : Git, Jenkins, Nexus, ...
Kafka	Hub de messagerie en cours de déploiement dans le cadre du projet FRVZ, est amener à devenir l'offre des échanges asynchrone du SI de l'Anah)
APIm	API Management en cours de déploiement
OwnCloud	Cloud Anah, outil de gestion de documents partagés

Les informations détaillées relatives aux spécifications applicatives, notamment les besoins métier en matière de disponibilité, les niveaux de criticité au sein de l'organisation, ainsi que les engagements associés (GTR, RTO et RPO), sont consultables dans un fichier en annexe du CCTP (2026-06_ANAH_Marché Infogérance_Etat des lieux des actifs Anah). Ce document de référence permet de disposer d'une vision complète et structurée des exigences attendues pour chaque service, facilitant ainsi leur gestion et leur exploitation dans le cadre de l'infogérance.

4. Composants managés

Certains middlewares ont été installés par le titulaire du précédent marché sur différentes machines.

Les middlewares les plus couramment déployés sont les suivants :

- Apache
- Docker
- HAProxy
- MariaDB
- MaxScale
- Nginx
- Pacemaker
- Pgpool
- Postfix
- PostgreSQL

La mise en œuvre de la haute disponibilité peut s'appuyer sur les composants suivants :

- HAProxy
- Pacemaker

Ces services doivent prioritairement faire l'objet d'une migration vers des services cloud managés, ou, à défaut, être repris et maintenus à l'identique par le titulaire entrant.

5. Périmètre en obsolescence

Application	OS obsolètes	OS arrivant prochainement à obsolescence	obsolescences middleware
FranceRenov	Non	Oui	Oui
SEL (HDS)	Non	Oui	Oui
AidesRenov	Non	Oui	Non
RNC	Oui	Oui	Oui

AnahFr	Non	Oui	Non
Extranet	Non	Oui	Oui
MAR	Non	Oui	Oui
SPRH	Non	Oui	Oui
Datafabrik	Non	Oui	Oui
Référentiel	Non	Oui	Oui
Forge - Airflow	Non	Non	Oui
Forge - Sentry	Non	Oui	Oui
Forge - SonarQube	Non	Oui	Oui
Forge - Jenkins	Non	Oui	Oui
Forge - Ansible	Non	Oui	Non
Forge - Mailpit	Non	Oui	Non
Forge - Gitlab	Non	Oui	Non
Kubernetes	Non	Oui	Oui
Forge - Nexus	Non	Oui	Oui

6. Indicateurs de performance

Le tableau ci-après présente les indicateurs actuellement suivis au sein de l'Anah :

Indicateur	Valeur
INCIDENTS	300
DEMANDES DE SERVICE	1500
CHANGEMENTS hors MEP	400
MISE EN PRODUCTION (MEP)	600

f. Les exclusions de périmètre

Sont exclus du marché les éléments suivants :

- La gestion du contenu
- Ma Prime Renov (PEGA) qui fait partie d'un contrat spécifique et dédié
- Le développement de nouvelles fonctionnalités
- La formation des utilisateurs finaux
- La gestion des postes de travail

IV. Exigences transversales

EXG-TRSV-001 : Localisation des équipes du TITULAIRE

Les équipes du TITULAIRE participant à la gestion de la plateforme de l'Anah doivent être localisées exclusivement en France Métropolitaine ou en Europe continentale (Union européenne et, le cas échéant, pays explicitement acceptés dans l'Espace économique européen (EEE)). Aucune activité relevant de la gestion de la plateforme (exploitation, supervision, administration, support, ingénierie, pilotage, etc.) ne doit être réalisée en dehors de cette zone géographique, sauf accord préalable, écrit et exprès de l'Anah.

La langue usuelle de travail est le français pour l'ensemble des échanges opérationnels et de pilotage lié à la gestion de la plateforme, incluant notamment :

- Les communications quotidiennes (tickets, emails, comptes rendus d'incidents, demandes de changement, etc.),
- Les réunions de suivi, comités opérationnels et comités de pilotage,
- La documentation de service (procédures d'exploitation, modes opératoires, rapports de service, plans d'actions, RCA, etc.).

Le TITULAIRE s'assure que ses collaborateurs disposent du niveau de français suffisant (oral et écrit) pour garantir la qualité et la fluidité des échanges avec les équipes de l'Anah. En cas de recours ponctuel à une autre langue (par exemple pour des échanges techniques avec un éditeur ou un tiers), le TITULAIRE demeure responsable de fournir à l'Anah une synthèse en français des informations pertinentes.

Toute évolution concernant la localisation des équipes (changement de pays, recours à un centre de services dans un autre État) est soumise à l'accord préalable et écrit de l'Anah et peut faire l'objet de mesures complémentaires (contractuelles, organisationnelles, de sécurité ou de conformité réglementaire).

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

EXG-TRSV-002 : Accès au réseau de l'Anah

Les équipes du TITULAIRE doivent travailler depuis leurs locaux ou depuis les locaux de l'Anah. Pour ceux qui travaillent depuis les locaux du TITULAIRE :

Un dispositif de contrôle d'accès doit être mis en place par le TITULAIRE, comprenant à minima :

- Une identification nominative des personnes autorisées (badge, liste nominative, etc.),
- Un contrôle des entrées et sorties (badges, registre, tourniquet ou équivalent),
- L'interdiction d'accès aux personnes non autorisées, sauf accompagnement et enregistrement préalable,
- Le cas échéant, des mesures complémentaires de sécurité physique (vidéosurveillance, verrouillage des locaux, etc.), conformément à la politique de sécurité applicable,
- Une revue périodique des accréditations et des habilitations est attendue de la part du TITULAIRE

Les équipements du TITULAIRE sont connectés au réseau de l'Anah via un accès sécurisé, mis en œuvre et détenu par le TITULAIRE. Cet accès sécurisé doit garantir :

- La confidentialité des échanges (chiffrement, tunnel VPN ou solution équivalente),
- L'intégrité et la disponibilité du trafic,
- La séparation des flux par rapport au réseau interne du TITULAIRE, conformément aux bonnes pratiques de sécurité et aux politiques des parties,
- La mise en place d'un contrôle d'accès avec une notion de MFA est aussi attendu de la part du TITULAIRE,
- La traçabilité des accès et des actions, ces éléments doivent être consultables sur demande,
- Les ressources intervenant sur le périmètre de l'infogérance doivent signer les documents relatifs à la conformité de l'Anah avant toute action

À ce titre, les exigences de sécurité physique et logique qui lui sont applicables doivent être respectées par le TITULAIRE et l'Anah, chacun pour ce qui le concerne, et font l'objet de contrôles et d'audits éventuels selon les modalités prévues au CCAP (article 12.8).

Dans le cadre du présent marché, le TITULAIRE doit aussi avoir la capacité de reprendre la gestion et l'administration du réseau sur les sites de l'Anah (OPERA, WOJO Port-Royal...) en complément du réseau Cloud. Cette dernière exigence sur l'administration des réseaux des sites Anah est souhaitable et n'est pas rédhibitoire.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

EXG-TRSV-003 : Fourniture des PC pour le personnel présent sur le site de l'Anah

L'Anah s'engage à provisionner, à ses frais, les postes de travail (matériel informatique, accessoires et logiciels de base nécessaires) **utilisés par les collaborateurs du TITULAIRE affectés à l'exécution du présent marché et dont la présence dans les locaux de l'Anah est requise**. Le matériel ainsi fourni demeure en toutes circonstances la pleine et entière propriété de l'Anah, aucune cession ni transfert de propriété implicite ou explicite n'étant consenti au TITULAIRE ou à ses collaborateurs.

Le poste de travail mis à disposition est placé sous la responsabilité opérationnelle du TITULAIRE pendant toute la durée d'affectation du collaborateur sur le marché. À ce titre, le TITULAIRE :

- Veille à la bonne utilisation du matériel fourni, dans le respect des règles et procédures de sécurité physique et logique définies par l'Anah,
- Met en œuvre toutes les mesures nécessaires pour prévenir la perte, le vol, la détérioration ou l'utilisation frauduleuse du poste de travail et des données qu'il contient,
- S'assure que ses collaborateurs n'installent pas de logiciels ou d'outils non autorisés et n'altèrent pas la configuration de sécurité mise en place, sauf accord préalable explicite de l'Anah,
- Informe sans délai l'Anah de tout incident affectant l'intégrité, la sécurité ou la disponibilité du matériel (perte, vol, casse, suspicion de compromission, etc.)

En fin de mission, en cas de remplacement de collaborateur, de résiliation ou d'expiration du marché, le TITULAIRE garantit la restitution en bon état de fonctionnement de l'ensemble des postes de travail et équipements associés mis à sa disposition (y compris accessoires, chargeurs, périphériques, badges éventuels), sous un délai maximum à définir dans les conditions particulières. La restitution s'effectue selon les modalités fixées par l'Anah (point de collecte, procédure de retour, effacement des données, etc.).

Le TITULAIRE est responsable de tout dommage, perte ou dégradation résultant d'une négligence, d'une mauvaise utilisation ou du non-respect des règles de sécurité par ses collaborateurs, sans préjudice des recours que l'Anah pourrait exercer.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

EXG-TRSV-004 : PC pour le personnel ne travaillant pas depuis le site de l'Anah

Le TITULAIRE doit fournir, à ses frais, l'ensemble des postes de travail nécessaires (matériel informatique, accessoires et logiciels de base) pour les collaborateurs affectés à l'exécution du présent marché. Lesdits postes de travail demeurent en toutes circonstances la propriété du TITULAIRE.

Les postes de travail mis à disposition des collaborateurs du TITULAIRE doivent, à minima :

- Respecter les standards de sécurité de l'Anah (antivirus, correctifs de sécurité à jour, chiffrement le cas échéant, gestion des accès, etc.),
- Être conformes aux exigences et politiques de sécurité définies par l'Anah, notamment en matière de sécurité logique, de protection des données et de contrôle des accès,

- Être configurés de manière à ne pas compromettre la sécurité des systèmes d'information de l'Anah.

À ce titre, le TITULAIRE :

- Met en place et maintient à jour les solutions de sécurité nécessaires (antivirus, EDR, filtrage, mises à jour systèmes et applicatives, etc.) sur les postes de travail utilisés dans le cadre du présent marché,
- Veille au respect, par ses collaborateurs, de la politique de sécurité de l'Anah et des procédures associées,
- Organise et dispense, pour son personnel intervenant dans le cadre du marché, des actions de sensibilisation et/ou de formation à la sécurité, couvrant notamment les risques de phishing, d'ingénierie sociale et les bonnes pratiques de cybersécurité,
- S'assure que ses collaborateurs n'installent pas de logiciels ou d'outils non autorisés susceptibles de contrevenir aux règles de sécurité de l'Anah.

Le TITULAIRE est responsable de tout incident de sécurité, dommage, perte ou dégradation imputable à un manquement à ces obligations (configuration des postes, respect des politiques de sécurité, comportement de ses collaborateurs), sans préjudice des recours que l'Anah pourrait exercer.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

EXG-TRSV-005 : Certifications attendues du TITULAIRE

Dans le cadre du présent marché, le TITULAIRE doit démontrer un niveau de maturité et de conformité élevé en matière de sécurité, de protection des données et de résilience, au travers des certifications et référentiels suivants :

- **Certification ISO 27001** : Le TITULAIRE doit être certifié ISO 27001 pour un périmètre pertinent au regard des services objets du marché (hébergement, infogérance, services cloud, etc.). La certification doit être en cours de validité pendant toute la durée du marché. Le TITULAIRE fournit, sur demande de l'Anah, le certificat à jour ainsi que le périmètre couvert. L'absence de certification ISO 27001 valide au moment de la remise de l'offre constitue un motif d'élimination de la candidature,
- **Certification / agrément HDS (Hébergeur de Données de Santé)** : Lorsque le périmètre du marché implique l'hébergement ou le traitement de données de santé au sens de la réglementation applicable, le TITULAIRE doit disposer d'une certification ou d'un agrément HDS couvrant ce périmètre.

Le TITULAIRE fournit son certificat HDS en cours de validité ainsi que le périmètre et les activités couvertes.

- **Conformité au cadre DORA (Digital Operational Resilience Act)** : La prise en compte du cadre réglementaire DORA et la capacité du TITULAIRE à s'y conformer, notamment en matière de résilience opérationnelle numérique, de gestion des risques TIC, de tests de résilience, de gestion des incidents majeurs et de reporting, est considérée comme un critère souhaitable et un élément de valorisation de l'offre. L'offre du TITULAIRE décrit, le cas échéant, son niveau d'alignement avec DORA, les mesures déjà mises en œuvre et les certifications, labels ou audits associés.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché. La perte ou le non-respect d'une des certifications peut entraîner la rupture du marché. (Cf. CCAP)

EXG-TRSV-006 : Intégration au réseau du TITULAIRE

Le TITULAIRE doit, dans le cadre de la migration des assets IT à partir du Data Center du TITULAIRE sortant, concevoir et mettre en œuvre une architecture d'intégration réseau garantissant la continuité et la reprise des réseaux de l'Anah, selon les principes suivants :

Le TITULAIRE doit reprendre et intégrer les plans d'adressage, les segments/réseaux (VLAN, VRF, sous-réseaux, etc.) et les règles de routage existants de l'Anah dans l'architecture Cloud, de manière à minimiser les impacts sur les applications, les interconnexions et les postes clients. Le TITULAIRE doit proposer des adaptations nécessaires pour garantir la sécurité du SI. Toute évolution doit être validée préalablement par l'Anah.

Pendant et après la migration, le TITULAIRE doit utiliser le réseau de l'ANAH comme réseau de transit principal pour l'ensemble des flux entre les ressources Cloud et les utilisateurs, systèmes et sites du TITULAIRE. Tout chemin alternatif (accès direct à Internet, peering tiers, etc.) est interdit sauf autorisation écrite préalable de l'ANAH.

Le TITULAIRE doit planifier et réaliser les bascules réseau (du DC vers le Cloud) de manière à garantir la continuité de service, en limitant les interruptions à celles préalablement approuvées par l'Anah. Les scénarios de bascule (DNS, routage, NAT, VPN, pare-feu, etc.) doivent être formalisés, testés et validés par l'Anah avant mise en production.

L'architecture d'interconnexion entre le Cloud et le réseau du TITULAIRE (tunnels VPN, liaisons dédiées, routage, points de sortie Internet, filtrage) doit respecter les politiques de réseau et de sécurité de l'Anah.

Tout changement d'architecture réseau lié à la migration (création/suppression de sous-réseaux, modification de plans d'adressage, nouvelles routes, ouverture/fermeture de flux) doit être soumis à l'approbation préalable de l'Anah et documenté dans le référentiel d'architecture et d'exploitation.

Le TITULAIRE doit fournir à l'Anah, avant la mise en production des environnements Cloud, la documentation détaillée de l'architecture réseau cible (schémas d'architecture, plans d'adressage, matrices de flux, configurations types des interconnexions) démontrant la bonne prise en compte et la reprise des réseaux de l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché. Le non-respect de cette exigence entraîne la tenue d'une instance de gouvernance adéquate.

EXG-TRSV-007 : Administration et exploitation sans accès aux données métiers

Le TITULAIRE doit assurer l'administration et l'exploitation de l'infrastructure Cloud sans accès aux données métiers et aux données de l'Anah.

Dans le cadre de la migration vers le Cloud et de l'infogérance associée, le TITULAIRE doit organiser ses services et son architecture de manière à garantir l'absence d'accès aux données métiers et aux données de l'Anah, selon les principes suivants :

- **Cloisonnement des responsabilités et des droits**

Le TITULAIRE limite strictement ses droits d'accès aux seules ressources nécessaires à l'administration technique de l'infrastructure Cloud (réseaux, systèmes, middleware, services managés), à l'exclusion de tout accès en lecture ou en écriture aux données métiers et aux contenus applicatifs de l'ANAH.

- **Séparation des environnements et des comptes**

Le TITULAIRE met en place une séparation claire entre :

- Les comptes et rôles d'administration de l'infrastructure Cloud, gérés par le TITULAIRE ;

- Les comptes et rôles d'accès aux données métiers, gérés exclusivement par l'Anah ou ses mandataires.

- **Mécanismes techniques de protection des données**

Le TITULAIRE met en œuvre des mécanismes techniques (chiffrement, gestion de clés, contrôle d'accès, journaux d'accès, bastions, etc.) permettant de s'assurer que les équipes du TITULAIRE ne peuvent ni consulter ni extraire les données métiers et les données de l'Anah.

- **Traçabilité et auditabilité**

Le TITULAIRE garantira la traçabilité de tous les accès aux environnements infogérés (journaux d'authentification, d'administration, d'accès aux ressources Cloud) et fournira à l'Anah, sur demande, les éléments permettant de vérifier l'absence d'accès non autorisé aux données métiers et aux données de l'Anah.

- **Procédures d'intervention encadrées**

Toute intervention susceptible d'exposer le TITULAIRE aux données métiers (par exemple, assistance aux opérations applicatives, analyse d'incident touchant les données) doit faire l'objet :

- D'une demande explicite et préalable de l'Anah ;
- D'une procédure spécifique validée par l'Anah (périmètre, durée, personnes habilitées, supervision, journalisation).

- **Engagement contractuel de non-accès**

Le TITULAIRE s'engage contractuellement à ne pas accéder aux données métiers et aux données de l'Anah, sauf instruction écrite et ponctuelle de ce dernier dans le cadre de procédures encadrées, et à informer immédiatement l'Anah de tout accès fortuit ou suspect à ces données.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché. Le non-respect répété de cette exigence et la non-mise en place d'un plan de remédiation entraîne la tenue d'une instance de gouvernance correspondante.

EXG-TRSV-008 : Pérennité des solutions logicielles utilisées

Le TITULAIRE peut utiliser les solutions logicielles de son choix pour assurer l'administration, l'exploitation et la supervision de l'infrastructure Cloud. Il est précisé que l'Anah utilise la solution logicielle Dynatrace et continuera à l'utiliser dans le cadre de ses besoins internes. Le TITULAIRE peut s'aligner avec ce choix et utiliser Dynatrace comme solution commune.

Il est aussi demandé au TITULAIRE de prévoir un plan de sorti vers une solution OpenSource dans le cas où la doctrine de l'état viendrait à changer. **Cette exigence de solution OpenSource est souhaitée et n'est pas rédhibitoire.**

Dans tous les cas de figures, le TITULAIRE précise les modalités contractuelles et financières dans sa réponse et respectera les critères suivants :

- **Responsabilité des licences**

Les licences, abonnements, droits d'usage et coûts associés à ces solutions logicielles sont entièrement à la charge du TITULAIRE et compris dans son offre, sauf disposition contraire explicitement prévue au contrat.

- **Pérennité des solutions**

Les solutions logicielles retenues par le TITULAIRE doivent être pérennes dans le temps, a minima pour toute la durée d'exécution du contrat. Le TITULAIRE garantit leur maintien en condition opérationnelle (support éditeur ou équivalent, mises à jour de sécurité, compatibilité avec l'infrastructure Cloud).

- **Évolutions ou remplacement de solutions**

En cas d'arrêt de commercialisation, de support ou de problème majeur affectant une solution, le TITULAIRE doit, à ses frais, proposer et mettre en œuvre une solution de remplacement équivalente ou supérieure, sans dégradation du service et sans coût supplémentaire pour l'Anah, après validation préalable par ce dernier.

- **Transparence**

Le TITULAIRE communique à l'Anah, sur demande, la liste des principales solutions logicielles utilisées pour l'exploitation de l'infrastructure Cloud, la version ainsi que leur mode de licence et de support.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

EXG-TRSV-009 : Capacité du TITULAIRE à manager les environnement Cloud

Le TITULAIRE doit démontrer sa capacité à administrer, exploiter et faire évoluer des infrastructures Cloud déployées chez les fournisseurs de services Cloud présents dans le marché UGAP. Ceci dans les différentes typologies de Cloud à savoir le Cloud Public, le Cloud Souverain et le Cloud certifié SecNumCloud.

Le TITULAIRE précise pour chaque typologie de Cloud :

- Le nombre de ressources qualifiées
- Le nombre de ressources certifiées
- Les certifications individuelles des ressources dont celui dispose
- La liste nominative des certifications d'entreprise détenues (titre, éditeur, niveau, date d'obtention, date d'expiration le cas échéant)
- Les projets similaires qu'il a réalisés au cours des cinq dernières années
- Des références clients

Les conséquences contractuelles et financières d'un non-respect des exigences ci-dessus sont traitées au CCAP.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

EXG-TRSV-010 : Présence sur site du SDM ou du responsable de l'exploitation

Le TITULAIRE s'engage à assurer, sur le site de l'Anah, une présence continue équivalente à 100 % d'un ETP, assurée par le Service Delivery Manager (SDM) et/ou le Responsable d'Exploitation. (Voir les exigences concernant l'attribution d'un SDM et d'un responsable d'exploitation)

À ce titre :

- Le TITULAIRE désigne nominativement un SDM et un Responsable d'Exploitation, intervenant en qualité d'interlocuteurs privilégiés de l'Anah pour le pilotage opérationnel et la qualité de service,
- La somme des temps de présence sur site du SDM et du Responsable d'Exploitation doit représenter, en permanence (hors congés légaux et absences dûment justifiées et anticipées), l'équivalent d'une présence à temps plein (100 %),
- Le planning de présence (répartition SDM / Responsable d'Exploitation, plages horaires de présence, modalités de remplacement en cas d'absence) est défini, validé et régulièrement mis à jour en concertation avec l'Anah,
- En cas d'absence simultanée imprévue du SDM et du Responsable d'Exploitation, le TITULAIRE met en place sans délai un dispositif de continuité, avec la désignation d'un remplaçant disposant de l'autorité et du niveau d'information nécessaires pour assurer la continuité du pilotage et de l'exploitation.

Tout manquement à cette obligation de présence peut faire l'objet de mesures correctives et, le cas échéant, de pénalités conformément aux dispositions prévues au marché.

Les conséquences contractuelles et financières d'un non-respect des exigences supra sont traitées au CCAP.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

100% de présence cumulé entre le SDM et le responsable d'exploitation à chaque COPIL.

Pénalités : Si taux de présence inférieur strict à 95%. (Cf. CCAP)

EXG-TRSV-011 : Continuité et adaptation du dispositif aux besoins de l'Anah

Le TITULAIRE décrit l'organisation, les moyens et les processus mis en œuvre pour garantir, pendant toute la durée du marché, un dispositif en permanence en phase avec l'activité de l'Anah, ses priorités et l'évolution de ses besoins.

Il s'engage notamment à :

- Assurer la continuité et le maintien du niveau de compétences de l'équipe affectée aux prestations, en garantissant une connaissance suffisante du contexte métier, du SI et des spécificités de l'Anah,
- Prendre en compte, qualifier, prioriser, traiter et suivre l'ensemble des demandes de l'Anah (prestations au fil de l'eau, prestations sur demande, projets particuliers), en garantissant leur traçabilité, leur pilotage et un reporting régulier,
- Respecter les calendriers et engagements de délais associés aux différentes prestations (interventions récurrentes, demandes ponctuelles, projets spécifiques), en alertant l'Anah en cas de risque de dérive et en proposant des plans d'actions correctifs,
- Ajuster sans délai le dispositif (organisation, ressources, compétences, profils mobilisés) en fonction des évolutions du projet, des demandes de l'Anah, des contraintes calendaires et des pics de charge, tout en maintenant le niveau de service attendu,
- Mettre en œuvre les outils, instances, indicateurs et procédures nécessaires pour piloter cette continuité (revues de charge et de capacité, comités de suivi, tableaux de bord, indicateurs de délai et de qualité), suivre l'évolution des compétences et mesurer l'efficacité de la prise en charge des demandes,
- Garantir des modalités d'intégration, de formation et d'accompagnement permettant à tout nouvel intervenant d'atteindre rapidement le niveau d'autonomie requis, sans impact sur les engagements de délais ni sur la qualité de service.

Le TITULAIRE doit démontrer sa capacité à maintenir dans la durée une équipe opérationnelle, compétente, dimensionnée et organisée de façon à respecter les calendriers, absorber les pics de charge et traiter efficacement les prestations sur demande comme les projets particuliers confiés par l'Anah.

Les conséquences contractuelles et financières d'un non-respect des exigences supra sont traitées au CCAP.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

V. Modèle de gouvernance

a. Exigences communes à toutes les phases

Les aspects contractuels des comités de pilotage, de suivi et opérationnel relèvent du CCAP ; le présent chapitre fixe leurs objectifs, livrables et modalités de fonctionnement.

GOUV-COMM-001 : Définition et mise en place d'un RACI

Dans le cadre de la réversibilité entrante comme de la réversibilité sortante, le TITULAIRE doit élaborer et maintenir à jour un RACI détaillé, clair et exhaustif, couvrant l'ensemble des activités liées à la réversibilité.

À ce titre, le TITULAIRE :

- Identifie, pour chaque activité, livrable et jalon du plan de réversibilité, les rôles et responsabilités (Responsable, Approbateur, Contributeur, Informé) des parties prenantes du TITULAIRE, du TITULAIRE sortant ou entrant et de l'Anah,
- Décline ce RACI sur l'ensemble des activités relevant :
 - Des instances de gouvernance,
 - Des livrables à produire,
 - Des actions prévues dans le plan de réversibilité entrante et sortante,

- Soumettre ce RACI à l'Anah pour revue, partage et validation formelle,
- Met à jour le RACI si besoin (évolution du périmètre, des organisations ou des responsabilités) et s'assurer que toute version révisée est communiquée, partagée et validée par l'Anah.

Le RACI validé constitue la référence opposable pour la répartition des rôles et responsabilités entre l'Anah et le TITULAIRE dans le cadre de la réversibilité entrante et sortante.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché. Le RACI doit être tenu à jour tout au long du marché.

GOUV-COMM-002 : Définition et mise en place d'indicateurs pour les instances de suivi

Le TITULAIRE met en place et maintient un dispositif de pilotage permettant de produire, consolider, analyser et présenter en COPIL, au minimum mensuellement, les indicateurs suivants :

Disponibilité & performance des services

- Taux de disponibilité par service et par plage horaire contractuelle (en %)
- Nombre et durée cumulée des indisponibilités par service
- Respect des engagements de performance (temps de réponse, débits, etc.) le cas échéant
- Respect des SLA & qualité de service

Taux de respect des SLA incidents (par criticité)

- Taux de respect des SLA demandes de service
- Taux de respect des SLA changements (y compris mise en production)
- Nombre de pénalités théoriques et appliquées (le cas échéant)

Réactivité & rétablissement (support & opérations)

- MTTA (Mean Time To Acknowledge) : délai moyen de prise en compte des incidents (par criticité)
- MTTR (Mean Time To Repair/Resolve) : délai moyen de rétablissement/résolution (par criticité)
- Taux d'incidents résolus dans les délais contractuels
- Taux de réouverture d'incidents

Backlog & flux ITSM

- Volume d'incidents ouverts / clôturés / en backlog (par criticité)
- Volume de problèmes ouverts / clôturés / en backlog
- Volume de changements planifiés / réalisés / en backlog (et reportés)
- Aged backlog : ancienneté des tickets en retard (par tranche : <30 j, 30-60 j, >60 j)

Sauvegardes & restauration

- Taux de succès des sauvegardes (par périmètre : serveurs, bases de données, applications, postes, etc.)
- Taux d'échecs récurrents (même source / même cible)
- Taux de restaurations testées avec succès (par mois / trimestre)
- Délai moyen de restauration sur tests (vs objectifs RTO/RPO)

Obsolescence & conformité technique

- Nombre et pourcentage de composants (OS, middlewares, bases, matériels, appliances, etc.) en situation de support normal / support étendu / hors support
- Nombre de vulnérabilités critiques et hautes en attente de remédiation (et délai moyen de traitement)
- Taux de conformité aux standards techniques et de sécurité définis par le Client (golden images, versions cibles, etc.)
- Liste des équipements et composants en obsolescence

Capacité & performance des infrastructures

- Taux d'utilisation CPU / RAM / stockage / réseau sur les principaux composants (moyenne, pic, tendance)

- Taux d'anticipation des saturations (alertes de seuil vs actions préventives)
- Projection de capacité à 3–6 mois (basée sur les tendances de consommation)
- Nombre d'incidents causés par une insuffisance de capacité

Cloud & coûts (FinOps)

- Coûts cloud mensuels par environnement (PROD / PREPROD / DEV / autres) et par service / application
- Répartition des coûts par type de ressource (compute, stockage, réseau, services managés...)
- Taux de ressources sous-utilisées / sur-provisionnées (zombies, instances surdimensionnées, volumes orphelins...)
- Gains réalisés via les optimisations (rightsizing, réservations, plans d'épargne, etc.)
- Éventuellement : empreinte carbone estimée liée à la consommation cloud, si pertinent pour le marché

Satisfaction des utilisateurs & qualité perçue (Optionnel)

- Score de satisfaction utilisateur (CSAT) sur le support / les principaux services
- Évolution du nombre et du type de réclamations
- Principales irritants et plan d'actions associé

Plan d'actions & amélioration continue

- Analyse des tendances sur indicateurs précités
- Détection et sur et sous-consommations
- Suivi du plan d'actions d'amélioration : actions ouvertes / clôturées / en retard
- Gains mesurés obtenus (sur les indicateurs ci-dessus)
- Propositions d'optimisation / d'innovation formulées par le Titulaire et décisions prises en COPIL

Les indicateurs sont fournis dans un tableau de bord standardisé, validé conjointement dans les 3 premiers mois du marché.

Les données sources doivent être traçables et auditables (export des outils ITSM, monitoring, outils de sauvegarde, outils FinOps, etc.). Les indicateurs sont présentés avec historique, au minimum sur 6 mois glissants dès que possible, et commentés (analyse des écarts, causes, impacts, plan d'actions). Le TITULAIRE fournit, à chaque COPIL, une synthèse exécutive (1 slide) mettant en évidence : points de vigilance, risques, décisions attendues, et arbitrages budgétaires éventuels.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché. Les indicateurs doivent à tout moment représenter ce qui est pertinent pour l'Anah.

GOUV-COMM-003 : Intervention en heures non ouvrées (HNO) sur demande de l'Anah

Le TITULAIRE met en place, pendant toute la durée du marché, un dispositif d'astreinte en heures non ouvrées (HNO), activable sur demande expresse de l'Anah, permettant d'assurer la prise en charge et le traitement des demandes spécifiques (mise en production, mise à jour, patching etc ...) sur les plages suivantes :

- Astreinte en soirée : du lundi au vendredi, de 18h00 à 22h00,
- Astreinte de nuit : du lundi au vendredi, de 22h00 à 08h00,
- Astreinte en HNO week-end : du samedi 08h00 au lundi 08h00,
- Astreinte en HNO jours fériés : sur l'intégralité des journées légales de jours fériés

L'astreinte n'est mise en œuvre qu'en cas de besoin, sur la base d'une demande formelle de l'Anah (bon de commande, ordre de service ou tout autre moyen prévu au marché), laquelle précise au minimum : la plage concernée, la période d'activation et, le cas échéant, le périmètre fonctionnel ou technique visé.

Le dispositif d'astreinte HNO doit garantir, pour chaque période activée :

- La disponibilité d'un interlocuteur qualifié (technique et/ou fonctionnel selon les périmètres du marché), joignable via les canaux définis au présent CCTP,
- Le respect des délais de prise en compte et de traitement définis pour les incidents et demandes critiques (SLA HNO) pendant la durée d'activation,
- La capacité à engager immédiatement les actions nécessaires à la résolution, à la mise en œuvre de contournements ou à la mobilisation des équipes étendues, le cas échéant

Le TITULAIRE décrit, dans son offre, l'organisation retenue pour l'astreinte HNO (ressources, modalités de mobilisation sur demande, délais de mise en place après demande de l'Anah, procédures d'escalade, etc.).

Les coûts associés à l'astreinte HNO sont explicitement chiffrés dans le bordereau de prix, en distinguant à minima, pour des astreintes activables sur demande de l'Anah :

- Le coût unitaire de l'astreinte sur la plage 18h–22h,
- Le coût unitaire de l'astreinte de nuit,
- Le coût unitaire de l'astreinte en HNO week-end,
- Le coût unitaire de l'astreinte en HNO jours fériés

Ces coûts sont réputés couvrir l'intégralité des charges liées à la mise en place et au fonctionnement de l'astreinte pendant la durée d'activation (mobilisation des ressources, organisation, outillage, astreinte passive et, le cas échéant, interventions actives dans la limite définie au bordereau de prix). Toute intervention au-delà des modalités prévues est rémunérée selon les conditions financières définies au marché.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Le TITULAIRE doit répondre à 90% des demandes de prestations en HNO.

GOUV-COMM-004 : Astreinte, supervision et intervention en heures non ouvrées 24/7 (HNO)

Le TITULAIRE doit mettre en place, pendant toute la durée du marché, un dispositif d'astreinte 24/7 permettant d'assurer la prise en charge et le traitement des incidents.

Le dispositif d'astreinte doit garantir, pour chaque période activée :

- La disponibilité d'un interlocuteur qualifié (technique et/ou fonctionnel selon les périmètres du marché), joignable via les canaux définis au présent CCTP à savoir téléphone, mail, outils mis en œuvre etc ...
- Le respect des délais de prise en compte et de traitement définis pour les incidents et demandes critiques (SLA HNO) pendant la durée d'activation,
- La capacité à engager immédiatement les actions nécessaires à la résolution, à la mise en œuvre de contournements ou à la mobilisation des équipes étendues, le cas échéant

Les coûts sont réputés couvrir l'intégralité des charges liées à la mise en place et au fonctionnement de l'astreinte pendant la durée d'activation (mobilisation des ressources, organisation, outillage, astreinte passive et, le cas échéant, interventions actives dans la limite définie au bordereau de prix). Toute intervention au-delà des modalités prévues est rémunérée selon les conditions financières définies au marché.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Le TITULAIRE doit être capable d'assurer une supervision et une intervention en 24/7.

b. Exigences pendant les phases de réversibilité

Les conséquences financières, pénalités et mesures contractuelles en cas de non-respect des obligations de réversibilité sont fixées au CCAP

GOUV-REV-001 : Modèle de gouvernance pendant la période de réversibilité entrante – Comité de suivi de réversibilité (COSUI)

Sur toute la durée de la phase de réversibilité entrante, le TITULAIRE assure l'instance « **Comité de suivi de réversibilité** » :

Attendus	Description
Objectifs	Piloter le quotidien de la transition opérationnelle et de la réversibilité entrante
Fréquence	Hebdomadaire / Jour et heure à fixer au moment du lancement de la réversibilité
Participants	➤ Pilote de réversibilité Anah ➤ Responsable de l'infrastructure Anah ➤ Responsable des équipes d'exploitation Anah ➤ Pilote de réversibilité du TITULAIRE ➤ Responsable des équipes d'exploitation du TITULAIRE ➤ SDM du TITULAIRE ➤ Pilote de réversibilité du TITULAIRE sortant ➤ Responsable des équipes d'exploitation du TITULAIRE sortant Ce dispositif peut être complété par d'autres intervenants en fonction du besoin.
Activités	➤ Suivi détaillé des phases 1 ➤ Suivi détaillé du plan de réversibilité (écarts de planning, actions bloquantes, dépendances ...) ➤ Gestion des incidents et des risques liés à la transition ➤ Coordination avec l'ancien prestataire ➤ Pilotage des actions techniques ➤ Suivi de la transmission documentaire depuis l'ancien infogérant et le TITULAIRE ➤ Suivi de la migration des actifs sur le nouvel hébergement ➤ Suivi de la reprise en exploitation ➤ Suivi des KPI opérationnels ➤ Suivi et mise à jour du RIDA ➤ Préparation du COPIL avec les éléments de décisions et d'arbitrages (Critères de prises de décisions)
Livrables	➤ Les supports de réunions devront être transmis sur le site Confluence de l'Anah 24h avant la date de COSUI. ➤ Comptes-rendus des comités de suivi ➤ RIDA

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long de la période de réversibilité entrante.

GOUV-REV-002 : Modèle de gouvernance pendant la période de réversibilité entrante – Comité de pilotage de réversibilité (COFIL)

Sur toute la durée de la phase de réversibilité entrante, le TITULAIRE doit assurer l'instance **Comité de pilotage de réversibilité**. Ceci est une instance décisionnaire qui permet de prendre les décisions nécessaires à la bonne conduite et la poursuite de la réversibilité. Elle est notamment engageante pour les parties.

Attendus	Description
Objectifs	Assurer le pilotage stratégique et contractuel de la réversibilité entrante
Fréquence	Mensuelle / Jour et heure à fixer au moment du lancement de la réversibilité
Participants	➤ DSI et DSI Adjoint de l'Anah ➤ Pilote de réversibilité Anah ➤ Responsable de l'infrastructure Anah ➤ Pilote de réversibilité du TITULAIRE ➤ SDM du TITULAIRE ➤ Pilote de réversibilité du TITULAIRE sortant Ce dispositif peut être complété par d'autres intervenants en fonction du besoin.
Activités	➤ Suivi des KPI de migration / réversibilité ➤ Suivi des SLA contractuels globaux (disponibilité par service, respect SLA, MTTA, MTTR, backlog incidents, changements, taux de succès des sauvegardes ...) ➤ Suivi des risques, des points de blocage et des plans de mitigations ➤ Revue et suivi des risques / activités liées à la sécurité SI ➤ Arbitrage sur des sujets pré-identifiés ➤ Validation et ajustement du dispositif ➤ Validation des livrables clés ➤ Validation des jalons clés
Livrables	➤ Les supports de réunions devront être transmis sur le site Confluence de l'Anah 24h avant la date de COFIL. ➤ Comptes-rendus des comités de suivi ➤ RIDA mis à jour ➤ Les livrables identifiées parmi ceux présents dans l'exigence décrivant l'ensemble des livrables attendus.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long de la période de réversibilité entrante.

GOUV-REV-003 : Modèle de gouvernance pendant la période de réversibilité entrante – Réunion de lancement et de clôture de la réversibilité

Le TITULAIRE s'engage au titre de la réversibilité entrante à réaliser une réunion de lancement au début de la phase 1. Il s'engage aussi réaliser une réunion de clôture à la fin de l'ensemble des phases de réversibilité.

Le TITULAIRE du présent marché présente avec le TITULAIRE sortant le plan de réversibilité prévu dans le détail, le mode de suivi et de transmission des éléments documentaires. Il présente aussi les engagements de chaque partie en fonction des périmètres contractuels. Un travail préparatoire est attendu avec l'Anah afin de figer ces éléments qui deviendront le fil rouge de la réversibilité.

La fin de la réversibilité est actée par la signature d'un PV de réception de Réversibilité signé par les trois parties à savoir l'Anah, le TITULAIRE du présent marché et le TITULAIRE sortant.

La réunion de clôture présente un bilan complet de celle-ci et présente si besoin un complément de plan d'action nécessaire à la bonne prise en main et à l'exploitation de l'infrastructure IT de l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long de la période de réversibilité entrante.

GOUV-REV-004 : Liste des documents attendus en fin de réversibilité

Durant la phase de réversibilité le TITULAIRE entrant doit récupérer de la part du sortant les documents suivants :

- I. Le Dossier d'Architecture Général contenant le design global du site d'hébergement qui propose une vision haut niveau de l'architecture dédiée à l'infrastructure d'hébergement
- II. Le Dossier d'Architecture Technique de chaque environnement
- III. Le Dossier de Spécification Techniques Détaillé de chaque environnement
- IV. Les PV de recette de migration
- V. Les PV de recette de Mis en production
- VI. Les Dossiers d'Exploitation
 - a. Composants de sécurité
 - b. Monitoring
 - c. Backup
 - d. PCA / PRA
 - e. Réseaux
 - f. Accès

Ces documents doivent être mis à jour par le TITULAIRE et stockés dans le partage Confluence dédié. Ces documents sont la propriété de l'Anah. Une architecture et une organisation type de cet espace de stockage est présentée par le TITULAIRE au démarrage de la phase 1 de réversibilité.

Les documents venant à manquer sont à signaler lors des COSUI. La liste des environnements est donnée dans les annexes de ce présent CCTP.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long de la période de réversibilité entrante.

c. Exigences pendant la phase de RUN nominale (post-réversibilité entrante)

GOUV-RUN-001 : Attribution d'un SDM (Service Delivery Manager)

Dans le cadre de la gouvernance du présent marché, il est demandé au TITULAIRE d'attribuer un Service Delivery Manager (SDM) dédié au marché.

Le SDM est responsable :

- Du suivi de la qualité de service et du respect des engagements (SLA, disponibilité, performance),
- De la gouvernance du contrat (préparation et animation des COMOP/COPIL, tenue des plans d'actions, gestion des risques et des escalades),
- De la coordination des équipes de delivery (exploitation, cloud, réseau, sécurité, bases de données, etc.) et de la bonne allocation des ressources nécessaires,
- De la gestion des incidents majeurs et des situations de crise (pilotage des cellules de crise, communication vers l'Anah, production et suivi des plans d'actions issus des RCA),
- Du reporting régulier vers l'Anah (rapports de service mensuels ou trimestriels, indicateurs de performance, synthèse des incidents et changements, suivi des actions d'amélioration),
- Le cas échéant, du suivi financier et FinOps du périmètre cloud (reporting de consommation, alerte en cas de dérive, recommandations d'optimisation des coûts),

- De la mise à jour du catalogue de services d'infogérance cloud et de la conformité du service vis-à-vis des exigences contractuelles et de sécurité.

Les livrables attendus du SDM à minima sont :

- Rapport d'exploitation
- Synthèse des incidents majeurs (RCA)
- Plan d'actions
- Suivi des SLA
- Suivi capacitaire et FinOps
- Suivi des risques

Cette liste peut être complétée par le TITULAIRE en fonction des besoins

Le SDM dispose d'une expérience significative en pilotage de contrats d'infogérance Cloud et de bonnes pratiques ITSM (ITIL). Il est stable sur le périmètre (remplacement encadré par un délai et une phase de transition définis au contrat) et disponible sur les horaires de service définis, avec participation obligatoire aux instances de gouvernance prévues dans le CCTP.

Le SDM doit assurer avec le responsable de l'exploitation une présence sur site Anah à 100% (l'un ou l'autre en fonction des contraintes).

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GOUV-RUN-002 : Mise en place d'une ressource « Responsable technique de l'équipe d'exploitation »

Dans le cadre de la gouvernance du présent marché, il est demandé au TITULAIRE un responsable technique de l'équipe d'exploitation dédié au marché.

Il est attendu de ce profil :

- De piloter l'équipe d'exploitation
 - Organise l'activité quotidienne (planning, priorisation, suivi des tâches)
 - Accompagne et fait monter en compétence les exploitants (coaching, formation, feedback)
- D'être le référent technique / expert métier de l'exploitation
 - Apporte un support technique de niveau avancé sur les incidents sensibles
 - Prend les décisions techniques d'exploitation (standards, procédures, outillage)
- De garantir de la qualité du run
 - S'assure du respect des procédures, des SLA et des bonnes pratiques d'exploitation
 - Valide les changements / mises en production du point de vue exploitation
- D'assurer la coordination et la communication
 - Fait le lien entre l'équipe d'exploitation, les équipes techniques (Dev, infra, sécurité) et les métiers
 - Produit un reporting synthétique sur l'activité de l'équipe (incidents, charges, risques)
- De valider l'exploitabilité avant la mise en production
 - Supervision active, sauvegarde validée, documentation à jour, procédure de rollback, consignes d'astreinte et de contrôle de capacité

Le responsable technique de l'équipe d'exploitation dispose d'une expertise approfondie sur les environnements techniques sous sa responsabilité (infrastructures, applications, outils d'exploitation) et des bonnes pratiques ITSM (ITIL). Il joue le rôle de référent pour l'équipe, en apportant un soutien technique de haut niveau et en garantissant la qualité du run au quotidien.

Il assure une présence stable sur le périmètre d'exploitation (remplacement encadré par un délai et une phase de transition définis au contrat) et reste disponible sur les horaires de service définis, y compris en participation organisée aux astreintes ou interventions planifiées si le contrat le prévoit. Il participe de manière obligatoire et régulière aux instances de suivi opérationnel et de gouvernance technique définies dans le CCTP, afin de partager la vision technique, remonter les risques, arbitrer les choix d'exploitation et suivre les plans d'actions d'amélioration continue.

Le « Responsable technique de l'équipe d'exploitation doit assurer avec le SDM une présence sur site Anah à 100%. (L'un ou l'autre en fonction des contraintes)

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GOUV-RUN-003 : Gouvernance Nominale – Comité Opérationnel

Sur toute la durée du marché, le TITULAIRE doit assurer la tenue d'un **Comité Opérationnel** :

Attendus	Description
Objectifs	Cette instance a pour objectif d'assurer un suivi rapproché de l'exploitation de l'infrastructure SI. Elle garantit la continuité du service et permet d'identifier rapidement des difficultés opérationnelles. Elle permet aussi d'assurer une gestion proactive de l'infrastructure.
Fréquence	Hebdomadaire (Jour et heure à définir en début de marché)
Participants	➤ Responsable de l'infrastructure Anah ➤ Responsable des équipes d'exploitation Anah ➤ SDM du TITULAIRE ➤ Responsable d'exploitation du TITULAIRE ➤ Référent technique du TITULAIRE D'autres profils pourront y participer en fonction des sujets et des besoins
Activités	➤ Revu des incidents de la semaine ➤ Suivi des problèmes et RCA (Root Cause Analysis) ➤ Suivi des changements CAB (Change Advisory Board) ➤ Etat de la plateforme ➤ Sécurité ➤ Actions ouvertes ➤ Revue des autres indicateurs de performances inhérents à cette instance D'autres sujets pourront y être abordés en fonction des besoins.
Livrables	➤ Comptes-rendus des comités Opérationnel ➤ RIDA mis à jour

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence et tenue des instances de gouvernance tout au long du marché.

GOUV-RUN-004 : Gouvernance Nominale – Comité de Suivi

Sur toute la durée du marché, le TITULAIRE doit assurer la tenue d'un **Comité de Suivi** :

Attendus	Description
Objectifs	Cette instance a pour objectif d'assurer le suivi opérationnel et contractuel du marché. Il permet entre autres le pilotage de la qualité de service de l'exploitation de la plateforme. Il permet aussi la gestion et le suivi des SLA en vue de préparer le COPIL.
Fréquence	Mensuelle (Jour et heure à définir en début de marché)
Participants	➤ Responsable de l'infrastructure Anah ➤ Responsable des équipes d'exploitation Anah ➤ SDM du TITULAIRE ➤ Responsable d'exploitation du TITULAIRE D'autres profils pourront y participer en fonction des sujets et des besoins
Activités	➤ Revue des faits marquants du mois (Incidents, CAB etc.) ➤ Etat de la plateforme et actions proactives à prévoir (Capacitaires, Gestion de l'obsolescence) ➤ Suivi des engagements contractuels et des SLA ➤ Revue et suivi des risques / activités liées à la sécurité SI ➤ Actions ouvertes ➤ Revue FinOps et optimisation associées ➤ Revue du RIDA ➤ Revue des autres indicateurs de performances inhérents à cette instance D'autres sujets peuvent y être abordés en fonction des besoins.
Livrables	➤ Comptes-rendus des comités de suivi ➤ RIDA mis à jour

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence et tenue des instances de gouvernance tout au long du marché.

GOUV-RUN-005 : Gouvernance Nominale – Comité de Pilotage

Sur toute la durée du marché, le TITULAIRE assure la tenue d'un **Comité de Pilotage** :

Le COPIL est une instance de gouvernance rassemblant les parties prenantes clés afin d'assurer le pilotage global du contrat et de la plateforme. Il a pour objectifs d'examiner de manière synthétique les résultats du trimestre (qualité de service, respect des engagements contractuels et des SLA, incidents majeurs, risques, plan d'actions), de valider les arbitrages nécessaires (priorisation des évolutions, moyens à mobiliser, ajustements contractuels éventuels) et de définir les orientations pour le trimestre à venir.

Attendus	Description
Objectifs	Instance décisionnaire, d'orientation stratégique et de revue contractuelle
Fréquence	Semestrielle (Jour et heure à définir en début de marché)

Participants	➤ DSI et DSI Adjoint de l'Anah ➤ Responsable de l'infrastructure Anah ➤ Le responsable des achats Anah ➤ SDM du TITULAIRE ➤ Responsable technique de l'équipe d'exploitation du TITULAIRE ➤ L'engagement manager du SOUMISSIONNAIRE Ce dispositif peut être complété par d'autres intervenants en fonction du besoin.
Activités	➤ Revue des faits marquants depuis le dernier COPIL ➤ Suivi des risques ➤ Suivi des KPI, des SLA et revue contractuelle ➤ Etat de la plateforme et actions proactives à prévoir ➤ Revue budgétaire du marché ➤ Suivi des dépenses Cloud ➤ Revue des décisions et des orientations à prendre ➤ Revue des autres indicateurs de performances inhérents à cette instance D'autres sujets pourront y être abordés en fonction des besoins.
Livrables	➤ Comptes-rendus ➤ RIDA mis à jour

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence et tenue des instances de gouvernance tout au long du marché.

GOUV-RUN-006 : Plan d'action en cas de non-atteinte des SLA

Dès lors qu'une SLA n'est pas atteinte, le TITULAIRE doit préparer un plan d'action avec un calendrier clair de mise en œuvre. Ce plan d'action est présenté et validé avec l'Anah à l'instance de gouvernance idoine.

Contrôle de l'atteinte des résultats :

☒ Engagement et réponse écrite

☐ Autre (Préciser)

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence et tenue des instances de gouvernance tout au long du marché.
Pénalités. : Décrits dans le CCAP.

Nature de la prestation :

☒ Prestation au forfait

☐ Prestation unitaire sur bon de commande

VI. Prestations attendues pendant les phases de réversibilités

Les réversibilités entrante et sortante suivent des schémas identiques. Ces schémas doivent être respectés et ajuster par le TITULAIRE en fonction des contraintes opérationnelles.

▪ Phase 1 : Phase de shadow :

- Prise de connaissance du contexte
- Audit complète de l'existant
- Observation en shadow des gestes d'exploitation et de RUN du TITULAIRE sortant
- Identification des points de vigilance, risques et adhérences critiques
- Organisation de sessions de transfert de connaissances (KT – Knowledge Transfer)
- Mise en place des accès et habilitations nécessaires
- Documentation initiale en reprise d'exploitation
- Lecture et prise de connaissance de l'intégralité de la documentation du TITULAIRE sortant
- Construction de la Landing Zone (LZ) sur l'environnement cible :

- Réseau, sécurité, IAM
- Standards d'architecture
- Supervision et logging
- **Phase 2 : Préparation de la migration**
 - Mise en conformité avec les exigences sécurité et réglementaires
 - Analyse des dépendances techniques
 - Identification des grappes d'applications indépendantes à migrer
 - Définition de la stratégie de migration :
 - Rehost, Replatform, Refactor (si applicable)
 - Élaboration du planning de migration :
 - Vagues de migration
 - Jalons et points de contrôle Définition des critères d'acceptation (Go / No-Go)
 - Préparation des environnements cibles (tests, pré-production, production)
 - Mise en place des outils de migration et de synchronisation des données
 - Élaboration du plan de communication (métiers, IT, parties prenantes)
 - Définition du plan de rollback
- **Phase 3 : Migration et de double run**
 - Migration des applications par vagues :
 - Déploiement sur environnement cible
 - Tests techniques et fonctionnels
 - Mise en place du double RUN :
 - Duplication des données (synchronisation temps réel ou différé)
 - Supervision des deux environnements
 - Suivi des performances et de la stabilité
 - Période d'observation VSR pour chaque vague de migration
 - Suivi des incidents
 - Correction des anomalies
 - Validation de la migration et migration des URL
 - Migration des URL / bascule DNS
 - Communication auprès des domaines, métiers ou utilisateurs finaux
 - Désactivation progressive des composants legacy
- **Phase 4 : Fin de réversibilité**
 - Validation de l'ensemble des migrations
 - Validation de la reprise en exploitation
 - Stabilisation de la plateforme cible
 - Transfert complet de responsabilité opérationnelle
 - Finalisation de la documentation :
 - Dossier d'exploitation
 - Architecture cible revue et validée
 - Procédures mises à jour
 - Bilan de la réversibilité (retour d'expérience, axes d'amélioration)
 - Signature du Procès-Verbal (PV) de fin de réversibilité
 - Décommissionnement des environnements sources (si applicable)

a. Exigences au titre de la réversibilité entrante

REV-ENT-001 : Réalisation d'un audit de l'existant

Dans le cadre de la reprise en exploitation de l'infrastructure IT de l'Anah, le TITULAIRE doit réaliser un audit technique complet des assets inclus dans le périmètre.

À cet effet, il doit : s'appuyer sur l'ensemble des éléments d'entrée fournis par l'Anah, exploiter les informations et livrables transmis par l'ancien infogérant, ainsi que l'ensemble de la documentation technique disponible (DAT, LLD, HLD, configurations, DEX, et tout autre document pertinent). Le TITULAIRE peut, le cas échéant, demander des compléments d'information au TITULAIRE sortant, dans le cadre et dans la limite des dispositions de réversibilité.

Cet audit, strictement limité aux aspects techniques de l'infrastructure (à l'exclusion de tout audit métier), servira de base à l'élaboration et à la structuration du plan de migration. Les livrables attendus sont :

- Le rapport d'audit
- L'architecture de l'Anah mise à jour et consolidé
- Une analyse des dépendances techniques et des flux inter-applicatifs, permettant d'identifier les points de vigilance pour la migration
- Un état des capacités et performances de l'infrastructure actuelle (dimensionnement, saturation, goulots d'étranglement)
- Des propositions d'amélioration sans remettre en cause le fonctionnement actuel de l'infrastructure (ex : règles firewall, optimisation ...)
- Un inventaire exhaustif et qualifié des actifs techniques, incluant leur état (obsolescence, support éditeur, conformité)
- Des préconisations techniques priorisées en vue de sécuriser la phase de migration (quick wins et chantiers structurants)
- Une contribution à la stratégie de migration, notamment via l'identification des prérequis techniques et des contraintes majeures

Il est rappelé que cet audit doit être réalisé dans les délais de la réversibilité.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Le rapport d'audit doit être un préalable aux travaux de migration.

REV-ENT-002 : Production d'un plan de réversibilité complète

Le TITULAIRE s'engage à élaborer, conjointement avec le TITULAIRE sortant, un plan de réversibilité complète couvrant l'ensemble des composants et services du périmètre infogéré.

Ce plan de réversibilité :

- Respecte strictement les phases, jalons et principes décrits dans le présent CCTP,
- Détaille les modalités de transfert des services, des connaissances, des outils et, le cas échéant, des données et configurations nécessaires à la continuité de service ;
- Précise les responsabilités respectives du TITULAIRE, du TITULAIRE sortant et de l'Anah à chaque étape de la réversibilité.

Le plan de réversibilité doit être partagé avec le TITULAIRE sortant et l'Anah, puis validé collégialement par les trois parties.

Toute évolution substantielle de ce plan doit être revue et approuvée dans les mêmes conditions.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Réalisation du plan de réversibilité sur le périmètre du marché.

REV-ENT-003 : Cartographie et pilotage des risques

Dans le cadre de la réversibilité, le TITULAIRE réalise, formalise et maintient une cartographie complète des risques. Cette cartographie doit permettre d'identifier, d'analyser et de prioriser les risques selon une approche structurée fondée sur l'identification des actifs, des menaces et des vulnérabilités, conformément aux bonnes pratiques du marché et aux référentiels reconnus tels que ISO 31000 et 27005, la méthode ANSSI EBIOS Risk Manager ainsi que les principes ITIL.

Le TITULAIRE doit évaluer les risques en termes d'impact et de probabilité, proposer un plan de traitement priorisé (réduction, transfert, évitement ou acceptation) et produire des livrables exploitables incluant une matrice de criticité, probabilité, une synthèse exécutive et un plan d'actions.

Il assure également le suivi et la mise à jour régulière de la cartographie, le pilotage des actions associées, ainsi que le reporting dans les instances de gouvernance, en intégrant notamment les enjeux de sécurité, de continuité d'activité, de dépendance aux fournisseurs et de souveraineté des données.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Suivi des risques tout au long de la phase de réversibilité entrante.

REV-ENT-004 : Production d'un plan de tests

Le TITULAIRE élabore, pour chaque application, un plan de tests couvrant les aspects techniques et de bout en bout.

Il met en œuvre un plan de tests techniques (performance, disponibilité, sécurité, connectivité, continuité/reprise) et en fournit les résultats à l'Anah et au TITULAIRE sortant. Les plans de tests fonctionnels sont produits par l'ANAH et exécutés par l'Anah, en présence du TITULAIRE sortant et du TITULAIRE du présent marché.

Le TITULAIRE du présent marché et le TITULAIRE sortant fournissent les moyens nécessaires, analysent les anomalies relevant de leur périmètre et mettent en œuvre les corrections permettant de satisfaire les critères de passage définis par l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Production d'un plan de tests validé par l'Anah lors de la phase de réversibilité entrante.

REV-ENT-005 : Suivi de la réversibilité

Le TITULAIRE doit produire, pour le suivi de la réversibilité, un tableau de bord de KPI avec à minima :

- Des indicateurs d'avancement (jalons, livrables, transfert de connaissances),
- Des indicateurs d'avancement de migration vers le Cloud choisi,
- Des indicateurs de qualité (qualité documentaire, qualité des inventaires, correction des anomalies),
- Des indicateurs d'impact sur la continuité de service (incidents, indisponibilités, respect des SLA),
- Des indicateurs de gouvernance (tenue des comités, suivi des décisions, traitement des risques et actions).

La liste définitive des KPI, leurs modalités de calcul, leurs seuils et leurs fréquences de reporting seront validés avec l'Anah et le TITULAIRE sortant lors du lancement de la phase de réversibilité. Une liste d'indicateurs est donnée en exigence GOUV-COMM-002.

Les différentes instances de gouvernance pendant cette phase de réversibilité sont précisées dans le chapitre des exigences des modèles de gouvernance.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence et tenue des instances de gouvernance avec les indicateurs demandés lors de la phase de réversibilité entrante.

REV-ENT-006 : Rappel des livrables attendus dans le cadre de la reprise en exploitation

Pendant la phase de réversibilité, le TITULAIRE prépare l'ensemble des documents et livrables cités ci-après pour la reprise de l'info-gérance qui est découpé en quatre phases.

Le passage d'une phase à l'autre est soumis à la validation par l'Anah des livrables suivants :

Phase 1 vers Phase 2 : Phase de shadow vers la préparation à la migration

- Dossier d'audit de l'existant et rapport associé
 - o Inventaire applicatif et infrastructure (CMDB de transition)
 - o Cartographie des composants (serveurs, bases, middleware, stockage, réseau, sécurité)
 - o Cartographie des flux et dépendances techniques majeures
 - o Synthèse des contrats/supports éditeurs, niveaux de service, contraintes réglementaires
 - o Analyse de conformité sécurité et réglementaire (écarts vs exigences cibles)
 - o Analyse de l'architecture existante (forces, faiblesses, obsolescence)
 - o Liste des risques, points de vigilance et adhérences critiques identifiés
 - o Recommandations préliminaires pour la migration et l'exploitation cible
- Comptes rendus de shadowing et de transferts de compétences
 - o Plan de transferts de connaissances (sessions réalisées, participants, supports)
 - o Procédures d'exploitation et de RUN observées et formalisées (ou complétées)
 - o Synthèse des écarts entre pratiques actuelles et pratiques cibles
 - o Procédures opérationnelles de base (gestion incidents, changements, sauvegardes, monitoring)
 - o Plan de continuité des opérations pendant la transition (RIDA à jour)
 - o Liste des accès et habilitations mises en place (et manquantes le cas échéant)
- Dossier d'architecture des landing zones
 - o Dossier d'architecture de la LZ (réseau, sécurité, IAM, standards d'architecture)
 - o Dossier de supervision et de logging (principes, outils, périmètre, dashboards prévus)
 - o Plan d'urbanisation de la LZ : périmètres, environnements (DEV/TEST/PRD), zones, comptes/projets
 - o Préparation d'un POV (Proof of Value) qui valide la conception et l'opérabilité des landing zones prévus et architecturés

Phase 2 vers Phase 3 : Préparation à la migration vers migration et double run

- Dossier POV (Proof of Value)
 - o PV de réalisation sans réserve qui valide le déclenchement des migrations
- Dossier de plan de migration
 - o Identification des grappes d'applications indépendantes
 - o Stratégie de migration : Lift & Shift, Rehost, Replatform ...
 - o Finalisation des choix techniques majeurs (outils, patrons de migration, prérequis ...)
 - o Planning de migration complet
 - o Plan des vagues et contenus
- Dossier d'architecture cible finalisé
- Dossier de conformité sécurité et de conformité réglementaire
- Plan de tests et d'acceptation
 - o Stratégie de tests techniques et fonctionnels par vague
 - o Jeux d'essais et responsabilités des tests (IT, métiers, intégrateurs)
 - o Critères de Go/No-Go formalisés par type de vague / application
- Plan de rollback par vague / par application
- Plan de communication (à réaliser par l'Anah)

Phase 3 vers Phase 4 : Fin de migration et fin de réversibilité

- PV de migration par vague
- PV de Go en production par vague
- Rapport de double run / VSR
- Plan de désactivation des composants legacy

- Rapport de fin de migrations
- Dossier de reprise en exploitation sur cible (Runbook cible)
- Dossier d'exploitation final
- Dossier d'architecture cible final
- Documentation technique et fonctionnelle à jour
- Dossier de transfert de responsabilité opérationnelle
- Rapport de bilan de réversibilité (RETEX)
- PV de fin de réversibilité
- Dossier de décommissionnement des environnements sources
- Références documentaires :
 - o HLD
 - o LLD
 - o DEX
 - o Procédure d'exploitation
 - o Matrice de flux
 - o Modèle IAM
 - o Stratégie de sauvegarde
 - o RACI
 - o Matrice d'escalade
 - o Inventaire CMDB
 - o ...

L'ensemble des livrables précités sont considérés pour la validation globale de la phase de réversibilité et de démarrage des opérations courantes du présent marché.

Ils sont stockés et organisés dans l'espace confluence propre à l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Livraison de l'ensemble des livrables de la liste à la fin de la période de réversibilité entrante.

REV-ENT-007 : Outils d'exploitation

Dans le cadre de la reprise des activités d'exploitation, le TITULAIRE doit mettre en œuvre le ou les outils d'exploitation de son choix, sous réserve de respecter les exigences techniques et organisationnelles définies dans le présent CCTP. À ce titre, il documente précisément les caractéristiques techniques des outils d'exploitation proposés (architecture, prérequis, périmètre fonctionnel, modalités d'exploitation courante, gestion des incidents et des changements, capacités d'automatisation, interfaces avec les autres briques du SI, modalités d'accès, etc.), conformément aux dispositions précisées plus haut dans le CCTP.

Le TITULAIRE veille à ce que ces outils couvrent l'ensemble des besoins d'exploitation de l'infrastructure et des services infogérés (supervision technique, gestion des incidents et des demandes, gestion des changements, gestion de la configuration et des actifs, planification des opérations récurrentes, reporting, etc.), et qu'ils s'intègrent de manière cohérente dans l'architecture cible.

Le détail des outils d'exploitation retenus, ainsi que leurs paramètres de configuration, leurs interfaces et leurs modes opératoires, sont formalisés et soumis à validation de l'Anah dans le cadre des phases de transition et des instances de gouvernance prévues au contrat.

Il est aussi demandé au TITULAIRE de prévoir un plan de sorti vers une solution OpenSource dans le cas où la doctrine de l'état viendrait à changer et dans le cas où les solutions adoptées sont soumises à des licences. **Cette exigence de solution OpenSource est souhaitée et n'est pas rédhibitoire.**

Le TITULAIRE s'engage à :

- Enlever les outils d'exploitation et les configurations associés du TITULAIRE sortant au cours de la migration des assets vers le Cloud cible.
- Garantir le bon fonctionnement de l'ensemble du dispositif d'exploitation, à en assurer le maintien en condition opérationnelle (MCO).

- Mettre à jour la documentation associée (documents d'architecture, dossiers d'exploitation, procédures, modes opératoires).
- Mettre à jour les modalités détaillées d'intégration avec le SI de l'Anah, de paramétrage des outils, de gestion des événements et opérations récurrentes, ainsi que de reporting.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Outils d'exploitation mises en œuvre.

REV-ENT-008 : Reprise des outils de supervision

Dans le cadre de la reprise des activités de supervision, le TITULAIRE devra mettre en œuvre la ou les solutions de supervision de son choix, sous réserve de respecter les exigences techniques et organisationnelles définies dans le présent CCTP. À ce titre, le TITULAIRE documentera précisément les caractéristiques techniques de la ou des solutions proposées (architecture, prérequis, modalités de collecte, types de sondes et de métriques, formats de logs, mécanismes d'alerting, interfaces de restitution, modes d'accès, etc.), conformément aux dispositions précisées plus haut dans le CCTP.

Par ailleurs, l'Anah disposant de sa propre solution de supervision, le TITULAIRE doit impérativement l'implémenter, la paramétrer et l'intégrer dans l'architecture de supervision cible. Il peut le cas échéant s'aligner avec le choix de l'Anah, à savoir l'utilisation commune de la solution Dynatrace.

Il est aussi demandé au TITULAIRE de prévoir un plan de sorti vers une solution OpenSource dans le cas où la doctrine de l'état viendrait à changer. **Cette exigence de solution OpenSource est souhaitée et n'est pas rédhibitoire.**

Il appartient notamment au TITULAIRE :

- De connecter les infrastructures et services infogérés à la solution de supervision de l'Anah,
- De définir et mettre en œuvre les seuils, alertes, tableaux de bord et rapports nécessaires au pilotage opérationnel et à la gouvernance,
- De veiller à la cohérence et à la non-redondance des dispositifs de supervision en cas de coexistence entre sa solution et celle de l'Anah (règles de priorité, périmètres respectifs, points de consolidation).

Le détail des configurations seront transmis par l'Anah et le TITULAIRE sortant au moment de la réversibilité. Le TITULAIRE du présent marché s'engage à garantir le bon fonctionnement de l'ensemble du dispositif de supervision (solutions de l'Anah et du TITULAIRE du présent marché), à en assurer le maintien en condition opérationnelle (MCO), ainsi que la mise à jour de la documentation associée. Les modalités détaillées d'intégration, de paramétrage, de gestion des alertes et de reporting font l'objet d'une validation avec l'Anah dans le cadre des instances de gouvernance prévues au contrat.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Mise en œuvre des outils de supervision

REV-ENT-009 : Reprise ou mise en place des outils de ticketing

Dans le cadre du présent marché, le TITULAIRE devra mettre en place un outil de ticketing complet, accessible en ligne de manière sécurisée. L'outil choisi doit être indiqué dans l'offre et accompagné d'une description détaillée de son mode de fonctionnement (principales fonctionnalités, gestion des profils et des droits, circuits de validation, modalités d'accès, sécurité, reporting, intégrations éventuelles avec d'autres outils, etc.).

L'Anah utilisant la solution JIRA pour le suivi de ses demandes, le TITULAIRE doit obligatoirement proposer une solution logicielle de ticketing compatible et connectable avec JIRA, permettant :

- À l'Anah de suivre en temps réel ou quasi-temps réel l'avancement des tickets,
- À l'Anah de créer des tickets dans JIRA avec une synchronisation automatique vers l'outil du TITULAIRE,
- De garantir un temps de prise en compte des demandes conforme aux SLA définis au présent CCTP.

À ce titre, le TITULAIRE peut proposer JIRA comme solution de ticketing commune.

Il est aussi demandé au TITULAIRE de prévoir un plan de sorti vers une solution OpenSource dans le cas où la doctrine de l'état viendrait à changer. **Cette exigence de solution OpenSource est souhaitée et n'est pas rédhibitoire.**

Le TITULAIRE entrant reprend l'intégralité des tickets ouverts et en cours de traitement par le TITULAIRE sortant. Il lui appartient de réintégrer l'ensemble de ces éléments (tickets, historiques, commentaires, pièces jointes, engagements associés) dans son propre outil de ticketing et/ou dans JIRA, de manière à garantir la continuité du suivi.

Le TITULAIRE doit, en outre, mettre à disposition de l'Anah des moyens de suivi en temps réel ou quasi-temps réel de l'avancement des demandes et des tickets en cours (accès en consultation à l'outil, tableaux de bord, rapports périodiques, etc.), conformément aux exigences de gouvernance et de reporting définies dans le présent CCTP.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Outil de ticketing déployé et fonctionnel.

REV-ENT-010 : Reprise des infrastructures

Dans le cadre du présent CCTP et de la reprise en infogérance, le TITULAIRE s'engage à reprendre l'intégralité de l'infrastructure VMWare existant vers l'hébergement cible qui est définie par l'Anah (Cloud / VMWare ou équivalent). Le TITULAIRE sortant met à disposition du TITULAIRE l'ensemble des VMs au format OVA/OVF.

À ce titre, il appartient au TITULAIRE :

- D'étudier et de documenter l'existant (inventaires, architectures, dépendances, contraintes techniques et de sécurité),
- De concevoir, documenter et construire les *landing zones* Cloud cibles, conformément aux exigences de l'Anah (sécurité, réseau, gouvernance, résilience, etc.) ;
- De planifier et de réaliser les migrations des composants et services depuis l'hébergement actuel vers les *landing zones* cibles, dans le respect des exigences de disponibilité et de continuité de service définies au contrat ;
- Enfin, de reprendre et d'assurer l'exploitation opérationnelle et le maintien en condition opérationnelle (MCO) des socles ainsi migrés, dans le cadre de l'infogérance.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

L'infrastructure de l'Anah est complètement reprise par le TITULAIRE

REV-ENT-011 : Reprise des accès et des habilitations

Dans le cadre de la réversibilité et de la reprise en infogérance de l'infrastructure de l'Anah, le TITULAIRE s'engage à reprendre l'intégralité des rôles, profils et accès existants au moment du lancement de la réversibilité, à l'exclusion des comptes, rôles et accès strictement spécifiques au TITULAIRE sortant.

Cela inclus aussi la reprise des accès VPN, bastions existants à iso périmètre et fonctionnalité. Le TITULAIRE peut aussi proposer des évolutions dans le cadre de l'audit de l'existant qui réalise pendant la phase de réversibilité.

Cette reprise s'effectue avec adaptation à la plateforme cible Cloud, ce qui peut nécessiter des ajustements (modification de rôles, de groupes, de permissions, de mécanismes d'authentification, de comptes techniques, etc.). Il appartient au TITULAIRE d'identifier, de prévoir et de présenter ces ajustements dans le cadre du plan de réversibilité et des dossiers d'architecture associés, pour validation par l'Anah.

Le TITULAIRE est responsable de la configuration et de la sécurisation de ces accès dans les environnements Cloud repris. Cette configuration fera l'objet de tests de bon fonctionnement, formalisés dans un procès-verbal (PV) de recette spécifique, validé par l'Anah. Toute anomalie ou divergence constatée doit être corrigée par le TITULAIRE dans des délais compatibles avec le planning de réversibilité.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

REV-ENT-012 : Ateliers de transfert de compétences

Le TITULAIRE devra établir une liste et un planning des transferts de compétences nécessaires à la bonne prise en main de l'infrastructure et des services infogérés. Cette liste est partagée avec le TITULAIRE sortant au démarrage de la phase de réversibilité.

La liste des transferts de compétences est validée collégialement par le TITULAIRE du présent marché, le TITULAIRE sortant et l'Anah, puis suivie dans le cadre des différentes instances de gouvernance dédiées à la réversibilité (comités de projet, comités de pilotage, etc.) jusqu'à la clôture de la phase de réversibilité.

Ces ateliers sont tracés dans un document de suivi contenant :

- Date
- Atelier
- Contenu
- Participants
- Supports
- Validation d'atteinte d'autonomie par le TITULAIRE du présent marché et le TITULAIRE sortant

Ce document est la source pour la signature du PV relatif à la réalisation des transferts de compétences.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Réalisation d'un ensemble de 10 (dix) ateliers de transfert de connaissances de deux heures chacun dans le cadre du forfait. Prévoir la possibilité d'en commander en complément en fonction du besoin.

REV-ENT-013 : Réalisation de POV sur une application significative

Le TITULAIRE réalise, en sortie de la phase 1 de la réversibilité, un ou plusieurs POV sur une ou des applications significatives. Ce ou ces POV ont pour objectif de valider la ou les landing zone(s) conçue en amont ainsi que les modalités de passage à la phase 2.

Dans ce cadre, il appartient au TITULAIRE de préparer en amont les différentes landing zones nécessaires (paramétrage, sécurité, connectivité, gouvernance, outillage, etc.), puis de mettre en œuvre le ou les POV sur un cas d'usage représentatif. Les résultats de ce POV doivent permettre de confirmer la pertinence du design de la landing zone, d'identifier les éventuels ajustements à apporter et de sécuriser le démarrage de la phase 2 de la réversibilité.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

POV réalisé et validé par l'Anah. Le TITULAIRE prévoit un ensemble de trois (3) POV dans le cadre d'un forfait. Il prévoit néanmoins la possibilité d'en commander en complément en fonction du besoin.

b. Exigences au titre de la réversibilité sortante

Toute sanction, résiliation ou conséquence contractuelle d'une non-conformité relève des stipulations du CCAP.

REV-SOR-001 : Délais de prévenance

La réversibilité sortante est déclenchée par l'Anah, sous réserve du respect d'un préavis de trois (3) mois avant la date souhaitée de passation. À compter de la notification de cette demande, le TITULAIRE met en œuvre et prépare l'ensemble des activités et les livrables liés à la réversibilité sortante, telles que définies au présent CCTP.

Pendant toute la durée de la réversibilité sortante et jusqu'à la stabilisation opérationnelle des services chez le successeur, le TITULAIRE est tenu :

- D'assurer un niveau de coopération minimale permettant l'accès aux informations, documentations, outils, données et personnels nécessaires à la reprise,
- De maintenir le service dans des conditions de qualité et de performance conformes aux engagements contractuels, sans dégradation injustifiée,
- De fournir l'assistance au successeur (technique, fonctionnelle et organisationnelle) requise pour permettre la bonne reprise et la stabilisation des services, dans des conditions raisonnables de délais et de moyens, telles que précisées au présent CCTP.

Dans l'hypothèse où le TITULAIRE n'est pas en mesure d'assurer la réversibilité sortante dans le délai imparti, il en informe sans délai l'Anah dès réception de ladite notification, en motivant les raisons de cette impossibilité et en proposant, le cas échéant, un plan d'actions alternatif.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence et tenue des instances de gouvernance tout au long du marché.

REV-SOR-002 : Préparation l'ensemble documentaires et mise à disposition au nouveau TITULAIRE

Dans le cadre de la réversibilité sortante, le TITULAIRE vérifie la complétude et la mise à jour des documents présents dans l'espace Confluence consacré à l'exploitation de l'infrastructure IT de l'Anah.

Le TITULAIRE s'engage à mettre à jour les documents afin de refléter fidèlement et exhaustivement la production au moment de la réversibilité. En outre, il s'engage jusqu'à la phase dite de « reverse shadow » à prendre en compte les modifications apportées et à en assurer la mise à jour documentaire sur les éléments concernés par le « reverse shadow ».

Le TITULAIRE s'engage aussi à transmettre les documents complémentaires demandés par le nouveau TITULAIRE dans la limite de ses engagements contractuels.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Les livrables listés sont mis à disposition du nouvel entrant.

REV-SOR-003 : Participation aux instances de gouvernance

Le SOUMISSIONNAIRE, sur la période de réversibilité s'engage à participer activement aux différentes instances de gouvernance et aux instances de cadrage propre à cette phase avec le nouveau TITULAIRE. Pour rappel, les instances de gouvernances et de cadrage pendant la phase de réversibilité sont décrites dans le chapitre II « Modèle de gouvernance ».

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Le TITULAIRE participe aux instances de gouvernance miroir lors de la réversibilité sortante.

REV-SOR-004 : Mise en place du mode « Shadow » et « Reverse Shadow »

Dans le cadre de la réversibilité, le TITULAIRE s'engage à mettre en place les éléments techniques nécessaires aux phases dites de « Shadow » et « Reverse Shadow ». À ce titre le TITULAIRE sortant configure les accès aux ressources IT de l'Anah au nouveau TITULAIRE.

Pendant la phase de « Shadow » les accès seront en « Lecture » et pendant la phase de « Reverse Shadow », ces accès seront en « Lecture / Ecriture ».

L'attribution des droits doit se faire en fonction des lots de reprises définis dans le plan de réversibilité. Par exemple, si la réversibilité comprend trois phases, les constituants techniques du phase 1 peuvent passer en « Lecture / Ecriture » tandis que les constituants des phases 2 et 3 resteront en « Lecture » pour le nouveau TITULAIRE.

Le SOUMISSIONNAIRE organise la transférabilité des comptes de gestions en respectant le plan de réversibilité vers le nouveau TITULAIRE. Cette transférabilité est validée lors des instances de suivi de réversibilité.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Le TITULAIRE prépare et participe de manière active à la mise en place des mode « shadow » et « reverse shadow » avec le nouveau TITULAIRE.

REV-SOR-005 : Attribution d'un pilote de réversibilité

Dans le cadre de la phase de réversibilité sortante du présent marché, il est demandé au TITULAIRE de désigner un Pilote de Réversibilité dédié, responsable de la bonne exécution de l'ensemble des activités de transition vers le TITULAIRE entrant et vers l'ANAH. Il est le point de contact du nouveau TITUALIRE. Ce rôle peut être cumulable avec les rôles de SDM et Responsable d'Exploitation citées plus haut dans le CCTP.

Le Pilote de Réversibilité est responsable en coordination du nouveau TITULAIRE des activités sous la responsabilité du TITULAIRE lors de cette phase notamment :

- Du suivi et de la coordination globale des activités de réversibilité (élaboration, mise à jour et suivi du plan de réversibilité, pilotage du planning, respect des jalons et engagements associés),
- De la coordination des équipes du TITULAIRE (exploitation, cloud, réseau, sécurité, bases de données, etc.) et de la mobilisation des ressources nécessaires à la bonne réalisation des transferts (connaissances, documents, configurations, outils, procédures),
- De la mise à disposition, de la complétude et de la qualité des livrables de réversibilité (inventaires d'assets, documentations techniques, dossiers d'exploitation, configurations, scripts, rapports de tests, PV de transfert, etc.),
- De la gestion des risques, des points de blocage et des dépendances liés à la réversibilité, ainsi que de la définition, du suivi et de la clôture des plans de mitigation associés,
- De la gestion des incidents et dysfonctionnements impactant la réversibilité, y compris l'escalade vers les niveaux appropriés, la coordination avec le TITULAIRE entrant et l'Anah, et la mise en œuvre des actions correctrices nécessaires,
- De la communication formelle et régulière vers l'Anah et le TITULAIRE entrant sur l'avancement de la réversibilité (reporting, tableaux de bord, indicateurs de progrès, suivi des jalons, synthèse des risques et actions),
- Le cas échéant, du suivi des engagements de niveau de service pendant la phase de réversibilité et de la gestion des éventuelles adaptations organisationnelles nécessaires (répartition des rôles, passage de relais progressif, ajustement des responsabilités).

Le Pilote de Réversibilité dispose d'une expérience significative en conduite de projets de transition et de réversibilité d'infogérance, incluant des environnements Cloud et hybrides, ainsi qu'une bonne maîtrise des bonnes pratiques ITSM (ITIL). Il est stable sur la durée de la réversibilité (tout remplacement étant encadré par un préavis et une phase de transition définis au contrat) et disponible sur les horaires de service définis, avec participation obligatoire aux instances de gouvernance et de pilotage dédiées à la réversibilité prévues dans le CCTP.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Le TITULAIRE doit mettre en place un pilote avec les connaissances de l'ANAH.

REV-SOR-006 : Suppression de l'ensemble des informations, données et documentations

Le TITULAIRE est tenu d'assurer la suppression définitive de l'ensemble des éléments (informations, données et documentations) placés sous sa responsabilité, après obtention de l'accord préalable exprès de l'ANAH, et de fournir un compte rendu détaillé de la destruction des informations, lesquelles seront évaluées par l'ANAH comme sensible.

La suppression des éléments sensibles doit être réalisée conformément aux procédures établies en coordination avec l'ANAH.

Le TITULAIRE, ses sous-traitants ainsi que l'ensemble de leurs intervenants s'engagent à respecter une stricte obligation de confidentialité et à ne divulguer, céder ou commercialiser, à quelque titre que ce soit, aucun des éléments traités par le système auprès de tiers.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Suppression de l'ensemble des éléments par le titulaire sortant.

VII. Catalogue de principaux services

Les fonctionnalités et exigences décrits ci-dessous sont à prendre en compte et à implémenter dans l'outil de ticketing qui est choisi par le TITULAIRE.

SRV-TSV-001 : Exploitation

Dans le cadre du marché, l'exploitation du SI fera l'objet de commandes récurrentes d'unités d'œuvre (UO) liées aux activités d'exploitation (applications, réseau, gouvernance, etc.).

Ces prestations d'exploitation sont déclenchées par bons de commande mensuels et ajustées au fil de l'eau en fonction des entrées et sorties d'assets IT dans le périmètre (ajouts, suppressions, optimisations). Le volume d'UO commandé chaque mois est ainsi recalibré pour refléter précisément le patrimoine technique à exploiter, tout en permettant une optimisation financière continue par le TITULAIRE.

Ainsi, le dispositif se rapproche d'un forfait d'exploitation, tout en restant fondé sur des commandes d'UO récurrentes et ajustables mois par mois, selon l'évolution du SI et des services associés.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

SRV-TSV-002 : Poste à pourvoir

L'Anah ne disposant pas à ce stade d'une vision exhaustive des évolutions potentielles de son système d'information, le TITULAIRE doit proposer un dispositif permettant de réaliser, sur devis, des prestations d'étude (technique, fonctionnelle, d'architecture, d'impacts) et/ou de mise en œuvre (build, intégration, migration, automatisation, etc.)

Ces prestations font l'objet d'une classification par complexité :

- Prestation simple : périmètre limité, impacts faibles, durée courte.
- Prestation de complexité moyenne : périmètre élargi, impacts modérés, plusieurs composants ou équipes concernés.
- Prestation complexe : périmètre étendu ou structurant, impacts significatifs sur l'architecture, l'exploitation ou la sécurité.

Pour chaque demande, le TITULAIRE remet un devis détaillé, comprenant à minima : la description du besoin, le niveau de complexité retenu, les hypothèses et le périmètre, les charges estimées, le planning prévisionnel et la liste des livrables. La remise des devis est encadrée par des SLA spécifiques de délai de réponse, différenciés selon le niveau de complexité (simple / moyen / complexe) et opposables au TITULAIRE.

Les prestations réalisées sur devis sont intégrées à la gouvernance du contrat : elles sont suivies dans les instances de pilotage (comités opérationnels, comités de projet, comités de pilotage) au même titre que les autres prestations. Les livrables (études, dossiers de conception, documentation d'exploitation, PV de recette, etc.) doivent respecter les exigences de qualité, de traçabilité et de documentation définies au marché.

Les prestations sur devis sont enfin soumises aux mêmes mécanismes de pénalités que les autres prestations du marché, tant pour le non-respect des SLA de remise des devis que pour le non-respect des engagements de délais et de qualité de réalisation.

Le TITULAIRE ne peut donc pas considérer ces prestations comme hors du périmètre contractuel, mais comme pleinement intégrées au dispositif de service et de gouvernance.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Délais de réponse avec un devis : 2 jours ouvrés pour une demande de complexité simple, 5 jours ouvrés pour une demande de complexité moyenne et 10 jours ouvrés pour une demande de complexité élevée.

a. Gestion des demandes

GST-DEM-001 : Niveau de priorité des demandes de services

Le TITULAIRE permet grâce à son outil de ticketing de créer et de suivre un ticket de service. Toutes les demande de changement doivent passer en CAB sauf celles qui bénéficient d'une validation automatique.

Une demande de service peut avoir plusieurs niveaux de criticité et doit respecter à minimas les niveaux suivants :

Priorité	Niveau	Description
P0	Très urgent	Demande critique métier qui nécessite un traitement immédiat. Cette demande peut être traitée par la validation hiérarchique adéquate et peut passer en CAB (Change Advisory Board) à postériori. Exemple : Demande d'ouverture de flux urgente / arrêt d'un service en production
P1	Urgent	Demande importante avec une forte contrainte temporelle.
P2	Standard	Demande normale.
P3	Faible	Demande non prioritaire.

La priorité des demandes peut être revue par le TITULAIRE et par le TITULAIRE avec la validation de l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEM-002 : SLA applicable sur les demandes de services

Le TITULAIRE doit respecter à minimas les délais de traitement décrits ci-dessous dans la gestion des demandes.

Priorité	Accusé réception	Prise en charge	Délais de réalisation
P0	15 minutes	30 minutes	Inférieur à 4 heures
P1	1 heure	2 heures	Inférieur à 8 heures
P2	4 heures	8 heures	Inférieur à 2 jours ouvrés
P3	8 heures	2 jours ouvrés	Inférieur à 7 jours ouvrés

En cas de changement de priorité les SLA correspondant au nouveau SLA sont appliqués à partir de l'instant du changement de priorité. En cas d'impossibilité, le TITULAIRE motive les raisons par écrit dans le ticket de suivi.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEM-003 : Services inclus dans l'exploitation

Voici une liste non exhaustive des demandes possibles. Le TITULAIRE complète cette liste avec les services qu'il juge utile. Cette liste est maintenue tout au long de ce présent contrat. Elle fait partie des livrables attendus dans le cadre de l'infogérance.

Toute modification de cette liste est notifiée par écrit à l'ANAH pendant l'exécution du contrat.

Titre	Description
Installation d'une application	Le TITULAIRE installe, configure, automatise (CD) et met en place la supervision d'une application. La procédure d'installation et de configuration sont fournies par l'ANAH ou par l'éditeur. Dans le cadre de cette demande, des tickets de création d'infrastructure doivent être créés.
Intégration d'application	Le TITULAIRE intègre une application existante dans le système d'information de l'ANAH, en assurant les raccordements aux référentiels (annuaire, SSO, supervision ...) et aux flux métier. Les spécifications d'intégration sont fournies par l'ANAH ou par l'éditeur. Dans le cadre de cette demande, des tickets de changements doivent être créés.
Exploitation d'une application	Le TITULAIRE assure l'exploitation courante d'une application déjà installée et configurée, incluant la surveillance de sa disponibilité, la gestion des incidents, l'application des correctifs et la réalisation des sauvegardes.
Mise en place d'un VPN	Le TITULAIRE configure et déploie un tunnel VPN entre deux sites ou vers des utilisateurs distants, en définissant les politiques de chiffrement, d'authentification et de routage associées. Les prérequis techniques et les exigences de sécurité sont fournis par l'ANAH.
Installation et exploitation d'un VPN	Le TITULAIRE installe, configure et exploite en continu une solution VPN, incluant la gestion du cycle de vie des certificats, la surveillance de la disponibilité des tunnels et l'application des mises à jour de sécurité
Configuration et exploitation du réseau	Le TITULAIRE configure et exploite les équipements et services réseau du périmètre défini par l'ANAH, en assurant la gestion des VLAN, des règles de routage, de la QoS et de la disponibilité.
Configuration et exploitation d'un routeur	Le TITULAIRE configure et exploite un ou plusieurs routeurs, en assurant la gestion des tables de routage, des protocoles dynamiques, des interfaces WAN/LAN et des mises à jour firmware.
Configuration et exploitation d'un firewall	Le TITULAIRE configure et exploite un ou plusieurs firewalls, en assurant la gestion des règles, la sécurité, des politiques NAT et des mises à jour de certificats. Toute modification de règle fait l'objet d'une demande de changement validée par l'ANAH.

Configuration et exploitation d'un système de détection d'intrusion	Le TITULAIRE configure et exploite un système de détection et de prévention d'intrusion (IDS/IPS), en assurant la mise à jour des signatures, l'analyse des alertes, le tuning des règles de détection et la remontée des événements de sécurité vers le puits de logs. Les politiques de détection sont définies en accord avec l'ANAH.
Installation et exploitation d'outils de surveillances	Le TITULAIRE installe, configure et exploite les outils de surveillance du système d'information (monitoring des ressources, disponibilité des services, métriques applicatives), en assurant la mise à jour des tableaux de bord. Les périmètres et seuils de surveillance sont définis par l'ANAH.
Installation et exploitation d'outils d'alertes	Le TITULAIRE installe, configure et exploite les outils de gestion des alertes, en assurant le paramétrage des seuils, des canaux de notification (email, SMS, ticketing) et des escalades. Les règles d'alerting et les astreintes sont définies en accord avec l'ANAH.
Installation et exploitation d'outils de puit de logs	Le TITULAIRE installe, configure et exploite la solution de centralisation et d'analyse des journaux d'événements, en assurant la collecte des sources, la définition des rétentions, la création des tableaux de bord et la gestion des accès aux logs. Les sources à collecter et les durées de rétention sont définies par l'ANAH.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEM-004 : Catalogue de demandes de services et priorité associées

Voici une liste non exhaustive des demandes possibles. Le TITULAIRE complète cette liste avec les services qu'il juge utile. Cette liste est maintenue tout au long de ce présent contrat. Elle fait partie des livrables attendus dans le cadre de l'infogérance.

Toute modification de cette liste est notifiée par écrit à l'ANAH pendant l'exécution du contrat.

Priorité	Type	Description
P1	PROV	Création / modification / suppression de VM.
P1	PROV	Création / modification / suppression d'un conteneur.
P1	PROV	Création / modification de bases de données (taille, édition, options).
P1	PROV	Création / modification de volumes de stockage, partages, buckets.
P1	PROV	Création / modification de composants réseau (load balancer, DNS, règles NSG, etc.).
P1	ACC	Création / modification / suppression de comptes techniques.
P1	ACC	Attribution / retrait de rôles ou groupes IAM.
P1	ACC	Gestion des accès temporaires / exceptionnels (justification + durée limitée).
P1	SAUV	Activation / modification de la sauvegarde sur une ressource.
P1	SAUV	Demande de restauration (fichier, base, VM) hors incident.
P1	SAUV	Modification de la rétention ou de la planification de sauvegarde.
P1	CONF	Modification de paramètres système standard (horaires de batch, logs, rotation...).
P1	CONF	Changement de configuration non intrusif et non stoppant (threshold d'alertes, tags, labels...).
P1	CONF	Ajout de monitoring / métriques / alertes sur une ressource.
P1	REP	Fourniture de rapports de consommation / coûts / FinOps.
P1	REP	Export de logs ou de données techniques.
P1	REP	Questions d'usage et demandes de conseil standard.

P2	AUT	Ajout d'un nouveau service au catalogue standard.
P2	AUT	Demandes d'accès aux documentations, modes opératoires, schémas.
P1	SERV	Installation et configuration d'une application à la demande de l'ANAH. Celui fourni le protocole d'installation.
P1	SERV	Exploitation d'une application
P1	SERV	Mise en place d'une supervision sur un composant donné
P1	RES	Analyse de performance d'une ressource (CPU, RAM, I/O, réseau).
P1	RES	Recommandations d'optimisation d'une ressource (rightsizing, tuning).
P1	RES	Gestion des incidents de capacité (saturation disque, mémoire, etc.).
P1	RES	Extension de capacité planifiée (scale-up / scale-out).
P1	SEC	Application de correctifs de sécurité (patch management).
P1	SEC	Gestion des vulnérabilités (scan, remédiation standard).
P1	SEC	Mise à jour des règles de sécurité (firewall, NSG, WAF).
P1	SEC	Analyse d'alertes de sécurité (niveau standard, hors incident majeur).
P0	INC	Prise en charge et résolution d'incident critique.
P1	INC	Prise en charge d'incident majeur ou dégradant.
P2	INC	Analyse post-incident (RCA – Root Cause Analysis).
P1	CHG	Gestion des changements standards (RFC standard).
P0	CHG	Gestion des changements urgents (hotfix, correctif critique).
P2	CHG	Participation aux comités de changement (CAB).
P1	EXP	Redémarrage contrôlé de services ou ressources.
P1	EXP	Relance de traitements batch ou jobs planifiés.
P1	EXP	Supervision quotidienne et traitement des alertes.
P1	DOC	Mise à jour de la documentation technique.
P2	DOC	Production de procédures / modes opératoires détaillés.
P2	DOC	Maintien des schémas d'architecture.
P1	PRA	Tests de restauration (PRA/PCA).
P1	PRA	Mise à jour des procédures de reprise.
P0	PRA	Activation du PRA en cas de sinistre.
P1	NET	Diagnostic réseau (latence, routage, connectivité).
P1	NET	Ouverture de flux (firewall, sécurité réseau).
P1	DATA	Opérations simples sur les données (import/export contrôlé).
P1	DATA	Support à la migration de données (niveau standard).
P2	FINOPS	Recommandations d'optimisation des coûts.
P1	FINOPS	Mise en place de budgets / alertes de consommation.

En cas de changement de priorité les SLA correspondant au nouveau SLA sont appliqués à partir de l'instant du changement de priorité. En cas d'impossibilité, le TITULAIRE motivera les raisons par écrit dans le ticket de suivi.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

b. Gestion des incidents

GST-INC-001 : Enregistrement et traçabilité de tout incident

Le TITULAIRE doit enregistrer systématiquement tout incident, quelle que soit son origine (détection automatique, signalement utilisateur, escalade interne), dans l'outil de gestion des services (ITSM) de référence définie contractuellement.

Chaque incident fait l'objet d'un ticket créé au moment de sa détection ou lors de son signalement. Ce ticket doit comporter à minima : l'identifiant unique, la date et l'heure d'ouverture, le canal de déclaration, la description de l'incident, le service ou système impacté, l'utilisateur ou l'entité affectée, et la personne ayant procédé à l'enregistrement.

Le TITULAIRE doit paramétrer ses outils de manière à avoir une création immédiate, voir automatisée d'un ticket contenant les informations essentielles et mis à jour tout au long du cycle de vie.

Le TITULAIRE garantit l'exhaustivité du registre des incidents sur toute la durée du contrat.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Intégration automatique des tickets via l'outil ITSM, taux de complétude des tickets attendu de 95% sur le mois et statistiques sur l'année. Taux d'exhaustivité des tickets 100%.

GST-INC-002 : Classification et priorisation des incidents

Le TITULAIRE doit appliquer une grille de classification et de priorisation des incidents, établie conjointement avec l'Anah en phase de lancement, fondée sur deux axes : l'urgence (délai acceptable d'interruption) et l'impact (périmètre fonctionnel et nombre d'utilisateurs affectés).

La grille retenue distingue au minimum quatre niveaux de priorité (P0 à P3).

À titre indicatif :

- P0 désigne un incident critique entraînant une interruption totale d'un service essentiel à l'activité de l'ANAH,
- P1 un incident criticité majeure avec dégradation significative,
- P2 un incident de criticité moyenne avec impact limité,
- P3 un incident de criticité faible sans incidence immédiate sur la production.

La classification est revue à tout moment si la situation évolue en cours de traitement. Le TITULAIRE documente la justification de la priorité attribuée.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Tout incident doit avec une priorité adéquate être renseignée dans l'outil ITSM.

GST-INC-003 : Respect des délais de prise en charge et de résolution (SLA)

Le TITULAIRE est tenu de respecter les niveaux de service (SLA) contractuels associés à chaque priorité d'incident, en matière de délai de prise en charge (MTTA) et de délai maximal de résolution (MTTR).

Le TITULAIRE doit respecter les délais de prise en charge et de résolution décrits ci-dessous.

Priorité	Délai de prise en charge	Délai maximal de résolution
P0	15 minutes	4 heures
P1	1 heure	8 heures
P2	4 heures	2 jours
P3	1 jour	7 jours

Si le délai maximal de résolution n'est pas tenu par le TITULAIRE, il avertit immédiatement l'Anah, active l'escalade et propose des solutions de contournement ou des solutions palliatives dans l'attente de la résolution définitive.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

95% des demandes respectent les critères de délais de prise en charge et les délais de résolution.

GST-INC-004 : Gestion de l'escalade

Le TITULAIRE doit disposer d'une procédure et d'une matrice d'escalade formalisée, fonctionnelle et hiérarchique, activée dès lors qu'un incident ne peut être résolu dans les délais impartis ou dépasse les compétences du niveau de support initial.

L'escalade fonctionnelle permet de transférer le ticket vers un niveau de support supérieur (N1 => N2 => N3 => éditeur) avec conservation de l'historique complet.

L'escalade hiérarchique implique la notification des responsables désignés côté TITULAIRE et côté Anah. Pour les incidents P0 et P1, une communication de situation (status update) doit être transmise à l'Anah toutes les heures jusqu'à résolution. Le TITULAIRE tient à jour un annuaire d'escalade actualisé et le soumet à la validation de l'Anah.

Le cas échéant les P0 déclenchent une cellule de crise portée par le TITULAIRE avec l'implication immédiate de l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-INC-005 : Communication et information des utilisateurs et de l'ANAH

Le TITULAIRE doit assurer une communication proactive et structurée vers les utilisateurs et les représentants de l'Anah tout au long du cycle de vie de l'incident.

Dès l'ouverture d'un incident P0 ou P1, une notification initiale à la direction informatique (SIDP) est envoyée aux parties prenantes identifiées dans un délai maximal de 30 minutes. Les mises à jour sont régulières, horodatées, et décrivent l'état d'avancement, les actions entreprises et l'estimation de rétablissement.

À la clôture, un message de résolution est transmis, indiquant la cause identifiée et les actions réalisées.

Le TITULAIRE propose un portail de suivi accessible à l'Anah permettant de consulter en temps réel l'état des tickets ouverts.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-INC-006 : Clôture et vérification de la résolution

Un incident ne peut être clôturé qu'après vérification du rétablissement effectif du service.

Pour les incidents de priorité P0, une validation formelle de l'Anah est obligatoire et doit être tracée dans les outils. Pour les incidents de priorité P1, une validation formelle par l'Anah ou par l'utilisateur concerné est requise. Le TITULAIRE s'assure dans tous les cas que la résolution est effective avant toute fermeture de ticket.

Pour les incidents de faible priorité (P2/P3), une période de surveillance de 24 heures peut être appliquée avant la clôture définitive. En l'absence de retour de l'utilisateur dans un délai défini contractuellement (par exemple 3 jours ouvrés), le ticket peut être clos, sous réserve d'une notification préalable à l'utilisateur.

Toute réouverture d'un incident clôturé dans les 5 jours ouvrés suivant sa fermeture est comptabilisée comme un incident non résolu aux fins du calcul des SLA et de la qualité de service.

Toutes les actions réalisées dans le cadre de la gestion des incidents (diagnostic, échanges, actions de résolution, validations, clôture, réouverture le cas échéant) doivent être tracées de manière systématique et exhaustive dans les outils prévus à cet effet.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-INC-007 : Reporting périodique sur les incidents

Le TITULAIRE doit produire un rapport mensuel de l'activité au niveau des incidents, transmis à l'ANAH dans les cinq jours ouvrés suivant la fin de la période.

Ce rapport présente à minima : le volume d'incidents par priorité, les taux de respect des SLA (MTTA et MTTR), les incidents récurrents, les incidents ayant nécessité une escalade, les tendances et anomalies observées, et les actions correctives engagées et les indicateurs précisés dans l'exigence GOUV-COMM-002.

Ce rapport alimente le comité de suivi et au besoin le comité de pilotage et sert de base à l'évaluation de la qualité de service.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

c. Gestion des problèmes

GST-PRB-001 : Identification et enregistrement des problèmes

Le TITULAIRE doit identifier les problèmes et les enregistrer dans l'outil ITSM, en les distinguant clairement des incidents. Un problème peut être identifié de manière réactive (à partir d'incidents récurrents ou d'un incident majeur) ou proactive (analyse des tendances, surveillance des infrastructures).

Un enregistrement de problème doit comporter : l'identifiant, la date d'ouverture, la description de la cause racine supposée ou avérée, les incidents associés, le service ou composant impacté, et la priorité attribuée. Le TITULAIRE est tenu d'ouvrir un enregistrement de problème dès lors qu'au moins deux incidents liés sont constatés sur un même composant dans une période glissante de 30 jours, ou à l'issue de tout incident P0.

Le TITULAIRE remet à l'Anah, au moins trimestriellement, une synthèse des problèmes potentiels identifiés de manière proactive, assortie de recommandations préventives. Cette activité est distincte du traitement réactif des incidents et fait l'objet d'un indicateur dédié dans le tableau de bord qualité.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-PRB-002 : Analyse des causes racines (Root Cause Analysis)

Le TITULAIRE doit conduire une analyse des causes racines (RCA) pour tout problème identifié, en s'appuyant sur des méthodes structurées et reconnues.

La RCA doit aboutir à l'identification de la ou des cause(s) racine(s), à la distinction entre cause immédiate, cause contributive et cause fondamentale, et à la formulation d'actions correctives. Pour les incidents P0, la RCA est transmise à l'Anah dans un délai de 5 jours ouvrés suivant la résolution de l'incident déclencheur.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-PRB-003 : Gestion des erreurs connues (Known Errors)

Le TITULAIRE doit maintenir une base des erreurs connues (KEDB - Known Error DataBase), accessible à l'ensemble des équipes de support, et mise à jour en continu.

Une erreur connue est constituée dès lors que la cause racine d'un problème a été identifiée, même si la solution définitive n'est pas encore déployée. La KEDB doit indiquer pour chaque entrée : la description du problème, la cause racine confirmée, les contournements (workarounds) disponibles, l'état d'avancement de la résolution et le calendrier prévisionnel de correction.

Cette base est partagée avec l'Anah dans un format consultable. Elle permet de réduire le temps de résolution des incidents futurs en fournissant aux techniciens une solution de contournement immédiatement exploitable.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-PRB-004 : Définition et suivi d'un plan d'actions correctives

Pour chaque problème, le TITULAIRE doit formaliser un plan d'actions correctives (Problem Resolution Plan) visant à éliminer la cause racine et à prévenir la récurrence.

Ce plan précise pour chaque action :

- L'intitulé,
- La nature (corrective, préventive, organisationnelle, technique),
- Le responsable désigné,
- Le délai d'exécution prévisionnel,
- Les critères de vérification.

Le plan est soumis à l'Anah pour information et peut faire l'objet d'un suivi lors des comités de pilotage. Le titulaire rend compte de l'avancement des actions à chaque comité de suivi opérationnel. Les actions non réalisées dans les délais prévus font l'objet d'une justification écrite.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-PRB-005 : Gestion proactive des problèmes

Le TITULAIRE doit mettre en œuvre une démarche proactive de gestion des problèmes, visant à identifier les risques et fragilités avant qu'ils ne donnent lieu à des incidents. Cette démarche repose sur l'analyse régulière des données de supervision, des journaux d'événements, des tendances d'incidents, et des alertes de capacité ou de performance.

Le TITULAIRE remet à l'Anah, au moins trimestriellement, une synthèse des problèmes potentiels identifiés de manière proactive, assortie de recommandations préventives. Cette activité est distincte du traitement réactif des incidents et fait l'objet d'un indicateur dédié dans le tableau de bord qualité.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-PRB-006 : Clôture des problèmes et capitalisation

Un problème est clôturé après élimination confirmée de la cause racine et vérification de l'absence de récurrence des incidents associés sur une période définie.

La clôture est formalisée dans l'outil ITSM avec un compte rendu de résolution documentant : la cause racine confirmée, les actions réalisées, les tests de vérification effectués, et les enseignements tirés (lessons learned). Ces éléments sont intégrés à la KEDB et, le cas échéant, à la base documentaire de l'ANAH. Le titulaire propose à minima un bilan annuel de la gestion des problèmes, permettant une capitalisation des connaissances et une amélioration continue du dispositif.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

d. Gestion des changements

GST-CHG-001 : Gestion du Changement

Un changement est un processus permettant une transition d'un état stable vers un nouvel état stable. Le rôle de la gestion des changements est d'assurer que toutes les modifications portées aux services du périmètre sont enregistrées puis évaluées, autorisées, classées par priorité, planifiées, testées, implémentées, documentées et revues selon des processus standardisés et formels. Ainsi, le processus de gestion des changements permet de contrôler l'exposition aux risques et l'impact et la sévérité des dysfonctionnements consécutifs à l'implémentation d'un changement.

Le périmètre inclut tout changement porté sur un service :

- Ajout, modification ou retrait d'un service ou d'un composant de service,
- Initié directement par le TITULAIRE ou par l'ANAH

La gestion des changements a un point d'entrée unique porté par le TITULAIRE et est impérativement gérée dans sa globalité au travers de l'outil de ticketing afin de pouvoir en garantir la traçabilité.

Dans le cas où une demande est particulièrement urgente, la procédure doit suivre le processus de gestion des changements urgents fourni par le TITULAIRE.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Les changements sont tous tracés et suivis dans le cadre de l'exploitation.

GST-CHG-002 : Acteurs des changements

Les principaux acteurs intervenant dans le processus de gestion des changements sont les suivants :

Acteur	Rôle
Initiateur	Individu initiateur de la demande en raison d'un problème rencontré ou d'un besoin d'évolution du service
Change Advisory Board (CAB)	Comité de pilotage des changements qui se réunit régulièrement (fréquence variable en fonction des services) afin d'évaluer, prioriser et planifier les changements à venir. Le CAB peut également prendre le rôle de comité d'urgence si une décision urgente doit être prise.
TITULAIRE	Groupe d'individus qui reçoivent et assigne la demande de changement
Équipe Développement	Groupe d'individus responsable du développement de la modification demandée.
Gestionnaire des changements	Individu responsable du filtrage, de l'acceptation et de la classification des demandes de changements. Il est également responsable de la planification et de la coordination de l'implémentation des changements
Exploitation	Groupe en charge de l'implémentation des changements

Il est de la responsabilité du TITULAIRE de :

- Rendre le processus le plus fluide possible, pour cela il doit obtenir de l'initiateur les informations les plus complètes possibles ;
- S'assurer que l'ensemble du processus est correctement tracé au travers de l'outil de ticket.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-CHG-003 : Classification des changements

Les changements peuvent concerner les services, applications, systèmes d'exploitation, bases de données, réseaux et toutes fonctions impactant le SI.

Il est de la responsabilité du TITULAIRE de catégoriser et de classer les changements.

Ils peuvent être de deux types :

- Changements à impact fonctionnel : ils concernent les modifications impactant directement les activités métiers et/ou utilisateurs finaux. Par exemple, l'ajout d'un menu sur une application ou la modification d'une règle de calcul d'un outil.
- Changements à impact technique : Ils concernent les modifications n'impactant pas directement les activités métiers et/ou utilisateurs finaux ou n'ayant qu'un impact technique. Par exemple, la modification de l'espace disque sur un serveur ou la modification du paramétrage d'un mot de passe sur un système.

Les changements sont classifiés en trois catégories :

- Changements standards : Il s'agit de modifications récurrentes parfaitement maîtrisées (exemple : déploiement de patches correctifs) et qui suivent donc un processus accéléré et standardisé de gestion des changements.
- Changements normaux : Ils concernent les modifications non standards dont l'urgence a été qualifiée de non-critique – car n'impactant pas de façon significative le maintien des niveaux de service - par le gestionnaire des changements.
- Changements urgents : Ils concernent les modifications dont l'urgence a été qualifiée de critique – car impactant les niveaux de service – par le gestionnaire des changements. Les changements demandés nécessitent une prise en compte immédiate et sont souvent consécutifs à un blocage des systèmes productifs. Un changement est considéré comme urgent lorsque celui-ci doit être implémenté dans un délai de deux (2) jours ouvrés.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-CHG-004 : Demande de changement

La demande de changement est initiée par les équipes du TITULAIRE ou par l'ANAH selon sa typologie (impact fonctionnel ou technique).

Les demandes de changements sont soumises par l'intermédiaire de l'outil de ticketing. Le TITULAIRE effectue une première analyse de la demande de changement visant à valider sa complétude.

La demande de changement doit contenir à minima les informations suivantes :

- Description de la modification demandée,
- Degré de priorité,
- Système concerné,

Suivant le type de demande il est aussi nécessaire d'avoir les informations suivantes :

- Estimation des ressources et du plan de déploiement nécessaires à la réalisation
- Evaluation des risques de mise en opération,
- Plan de test,
- Plan de retour arrière en cas de problème suite à la mise en opération,
- Délais estimés de réalisation, depuis la validation du changement jusqu'à la date de mise en opération,

La base des changements normaux est revue de manière hebdomadaire par le CAB qui validera individuellement chaque changement ainsi que les éléments suivants :

- Disponibilité des ressources pour réaliser les changements,
- Urgence et délai de traitement de la demande,
- Impacts techniques sur les autres modifications en cours.

Dans le cas où la demande de changement est jugée incomplète, elle est renvoyée par le TITULAIRE à l'initiateur. L'initiateur est alors notifié et peut procéder aux ajustements nécessaires avant de soumettre à nouveau sa demande.

Le TITULAIRE attribue également une priorité au changement et le soumet au gestionnaire de changement.

À réception de la demande, le gestionnaire des changements réévalue la priorité du changement :

- S'il estime que le changement nécessite d'être traité au plus vite, le processus de gestion des changements urgent est déclenché ;
- Si le changement est considéré comme standard, la demande est redirigée vers l'équipe responsable de sa mise en œuvre (en général l'Exploitation) pour action ;
- Si le changement est considéré comme normal, son impact (High, Medium, Low) ainsi que l'effort nécessaire à sa mise en œuvre sont évalués.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect des processus et des attentes sur la durée du marché.

GST-CHG-005 : Comité d'approbation des changements (CAB)

Le TITULAIRE met en place à intervalle régulier des Comités d'approbation des changements (CAB).

Les changements prêts à être mis en place sont revus et validés lors du CAB. Le planning et les ressources nécessaires sont alors validés.

Pour les changements les plus complexes, un plan de déploiement est présenté et validé en séance.

Le gestionnaire des changements et les équipes d'Exploitation sont informés de la date et des modalités de mise en production du changement.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Les CAB sont tenus régulièrement et font l'objet de CR validé par l'ANAH.

GST-CHG-006 : Revue post-implémentation

Le TITULAIRE doit réaliser, pour chaque changement mis en production, une revue post-implémentation formelle comprenant au minimum les éléments suivants :

- Collecter et analyser les informations clés relatives au changement (objectifs, périmètre, planning, risques identifiés, parties prenantes concernées).
- Évaluer les résultats obtenus par rapport aux objectifs initiaux (qualité, coûts, délais, impacts opérationnels) et vérifier le respect du processus de gestion des changements.
- Recenser les incidents, écarts et non-conformités, en identifier les causes racines et proposer des actions correctives et préventives documentées.
- Organiser une séance de retour d'expérience avec les équipes et parties prenantes concernées, afin de valider les constats et les enseignements.
- Produire un rapport formel de revue post-implémentation, incluant les leçons apprises et des recommandations d'amélioration pour les changements futurs, et le soumettre à l'instance de gouvernance / au client pour validation.

Le TITULAIRE doit fournir, dans son offre, la description détaillée de sa méthodologie et des livrables associés à cette revue post-implémentation.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

e. Gestion des configurations

GST-CONF-001 : Mise en place et tenue d'une base de données des configurations

Le TITULAIRE doit mettre en place, alimenter et maintenir à jour une base de données des éléments de configurations (CMDB), constituant la référence unique des composants du SI infogéré de l'ANAH.

La CMDB recense l'ensemble des éléments entrant dans le périmètre du marché : équipements physiques (serveurs, postes, équipements réseau), composants logiciels (systèmes d'exploitation, middlewares, applicatifs), services IT et contrats associés. Elle est hébergée dans l'outil ITSM de référence et est accessible en consultation à l'ANAH à tout moment.

Le TITULAIRE garantit que la CMDB est tenue en permanence à jour, réconciliée régulièrement avec l'état réel du parc, et intégrée aux processus de gestion des incidents, des changements, de la supervision et des actifs, de sorte que toute évolution sur l'un de ces processus se répercute sans délai dans la CMDB et réciproquement.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-CONF-002 : Identification et classification des éléments de configuration

LE TITULAIRE doit appliquer une nomenclature et une taxonomie des éléments de configurations, validée avec l'Anah en phase de lancement, permettant une identification non ambiguë et une classification cohérente de l'ensemble des éléments de configuration.

La classification distingue au minimum les catégories suivantes :

- Infrastructure (matériel, réseau, stockage),
- Logiciel (système, applicatif, licence),
- Documentation technique,
- Contrat tiers.

Chaque élément de configuration se voit attribuer un identifiant unique pérenne, non réutilisable après suppression.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-CONF-003 : Contrôle des modifications apportées aux éléments de configuration

Toute modification d'un élément de configuration : création, mise à jour, suspension ou suppression doivent faire l'objet d'un enregistrement tracé dans la CMDB, lié au changement ou à l'incident qui en est à l'origine.

Aucune modification d'un élément de configuration ne peut être opérée sans qu'une demande de change ait été préalablement approuvée selon le processus de gestion des changements détaillé ci-dessus. La CMDB conserve l'historique complet des états successifs de chaque élément, permettant un retour à un état antérieur en cas de besoin. Toute discordance constatée entre l'état réel d'un composant et son enregistrement en CMDB est traitée comme une anomalie et fait l'objet d'un ticket de régularisation.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-CONF-004 : Gestion des licences et des actifs logiciels

Le TITULAIRE doit assurer le suivi des licences logicielles associées aux composants infogérés, en veillant à la conformité permanente entre les droits d'usage contractés et les déploiements effectifs.

Le TITULAIRE alerte l'Anah dès lors qu'un risque de sous-licenciement ou de sur-licenciement est détecté, ou lorsqu'une échéance contractuelle approche à moins de 90 jours, à moins d'un mois, à moins d'une semaine et à une journée.

Un bilan annuel de la gestion des actifs logiciels est remis à l'Anah, servant de base aux décisions de renouvellement ou de rationalisation.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-CONF-005 : Reporting périodique sur la gestion des configurations

Le TITULAIRE produit un rapport semestriel sur l'état de la CMDB et la qualité de la gestion des configurations, transmis à l'ANAH dans les dix jours ouvrés suivant la fin de la période.

Ce rapport présente à minima :

- Le nombre d'éléments de configuration actifs par catégorie
- Le taux de conformité de la CMDB,
- Les résultats des audits conduits sur la période,
- Les évolutions significatives du parc (ajouts, retraits, mises à jour majeures),
- Le bilan du suivi des licences,
- Les actions de mise à jour engagées.

Il est présenté lors du comité de pilotage semestriel et constitue un indicateur de maturité du dispositif d'infogérance.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

f. Gestion des déploiements

GST-DEP-001 : Politique de gestion des versions

Le TITULAIRE définit et applique une politique formalisée de gestion des versions logicielles, couvrant l'ensemble des composants applicatifs et systèmes entrant dans le périmètre du marché.

Cette politique précise les règles de nommage et de versionnement (majeur, mineur, correctif), les critères de déclenchement d'un déploiement, les environnements concernés (développement, recette, préproduction, production), ainsi que les responsabilités associées à chaque étape du cycle de vie d'une version.

Elle est formalisée dans un document de référence soumis à validation de l'Anah au plus tard à l'issue de la phase de lancement du marché.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-002 : Gestion des environnements et séparation des niveaux

Le TITULAIRE assure la mise en place et le maintien d'une chaîne d'environnements distincts et étanches, garantissant qu'aucune version logicielle n'est déployée en production sans avoir été préalablement validée dans les environnements intermédiaires.

La chaîne comprend au minimum un environnement de recette (tests fonctionnels), un environnement de préproduction (tests de non-régression, tests de charge) et l'environnement de production. Le TITULAIRE garantit la représentativité de l'environnement de préproduction par rapport à la production, notamment en termes de configuration, de volumétrie de données et de paramétrage.

Le TITULAIRE propose un mode de fonctionnement où la création d'un environnement peut être complètement automatisé.

Toute dérogation à ce principe fait l'objet d'une demande d'autorisation écrite auprès de l'ANAH.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-003 : Procédure de mise en production

Le TITULAIRE applique une procédure de mise en production formalisée, validée par l'Anah, pour tout déploiement d'une nouvelle version ou d'un correctif en environnement de production.

Cette procédure décrit à minima :

- Les prérequis au déploiement (tests réalisés, critères de sortie de recette, validation fonctionnelle obtenue),
- Le séquençement des opérations techniques,
- Les contrôles de bon fonctionnement post-déploiement,
- Les acteurs impliqués et leurs rôles respectifs,
- La fenêtre de déploiement autorisée.

Le TITULAIRE doit valider l'exploitabilité avant la mise en production en s'assurant que :

- La supervision active des environnements,
- La procédure de sauvegarde est bien respectée,
- La documentation est à jour,
- La procédure de rollback est bien documentée,
- Les consignes d'astreinte et de contrôle de capacité sont bien définis.

Toute mise en production est associée à une demande de changement approuvée selon le processus de gestion des changements décrit ci-dessus.

Le TITULAIRE remet à l'Anah un compte rendu de mise en production dans les 24 heures suivant l'opération.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-004 : Planification et fenêtres de déploiement

Le TITULAIRE établit, en accord avec l'Anah, un calendrier prévisionnel des déploiements planifiés, mis à jour mensuellement et intégré au plan de gestion des changements. Les déploiements en production sont réalisés dans des fenêtres de maintenance définies contractuellement, en dehors des heures de forte utilisation du système d'information de l'ANAH.

Pour les déploiements susceptibles d'entraîner une interruption de service, même partielle, le TITULAIRE notifie l'Anah et les utilisateurs concernés au minimum cinq jours ouvrés à l'avance.

Les déploiements d'urgence (correctifs de sécurité critiques) font l'objet d'une procédure accélérée définie contractuellement, avec information immédiate de l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-005 : Tests et critères de validation avant mise en production

Le TITULAIRE est responsable de la conduite des tests nécessaires à la validation de chaque version avant son passage en production, et s'assure que les critères de sortie sont atteints avant tout déploiement.

Les tests à réaliser comprennent au minimum :

- Les tests unitaires et d'intégration,
- Les tests fonctionnels en environnement de recette,
- Les tests de non-régression,

Et, pour les versions majeures ou les composants critiques :

- Des tests de charge et de performance.

Les résultats de tests sont documentés et archivés dans l'outil ITSM. Aucun déploiement en production ne peut intervenir si les critères de validation ne sont pas intégralement satisfaits, sauf dérogation formelle accordée par l'Anah par écrit.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-006 : Plan de retour arrière (Rollback)

Pour tout déploiement en production, le TITULAIRE contribue à la préparation et documentation d'un plan de retour arrière (rollback plan), activable par l'Anah dans des délais définis et garantissant le rétablissement de la version antérieure en cas d'échec ou d'incident post-déploiement.

Ce plan précise :

- Les conditions de déclenchement du rollback,
- Le séquençage des opérations de retour arrière,
- Le délai maximal de retour à l'état stable antérieur,
- Les tests de vérification à conduire après restauration.

Pour le périmètre applicatif, le plan de retour arrière est élaboré par les équipes en charge de chaque domaine applicatif concerné et soumis à la validation formelle du TITULAIRE avant tout passage en production, qui s'assure de sa complétude et de sa faisabilité technique.

Le plan de rollback est testé périodiquement, au minimum une fois par an, et son résultat est consigné dans un rapport transmis à l'Anah. Pour les déploiements majeurs, le TITULAIRE maintient la version précédente disponible pendant une durée minimale définie contractuellement.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-007 : Gestion des correctifs de sécurité (Patch Management)

Le TITULAIRE assure une veille active sur les vulnérabilités affectant les composants du périmètre infogéré et met en œuvre une politique de gestion des correctifs de sécurité garantissant l'application des patches dans des délais proportionnels à la criticité de la vulnérabilité.

Les délais d'application sont définis selon le niveau de criticité de la vulnérabilité, en référence aux scores CVSS (Common Vulnerability Scoring System) :

Vulnérabilité	CVSS	Délai d'application du patch
Faible	<4	Intégré au cycle de maintenance standard
Moyenne	4-6.9	30 jours maximum
Haute	7-8.9	7 jours maximum
Critique	≥9	72 heures maximal

Chaque application de correctif suit la procédure de mise en production définie en CAT-GSTDEP-003. Le TITULAIRE produit mensuellement un état du niveau de patching du parc, transmis à l'ANAH.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-008 : Traçabilité et archivage des versions déployées

Le TITULAIRE maintient un registre des versions déployées en production, accessible à l'ANAH, constituant la référence opposable de l'état logiciel du SI infogéré à tout instant.

Ce registre indique pour chaque composant :

- La version courante en production,
- La date de déploiement,
- Le changement associé,
- Les versions antérieures archivées et leur date de retrait.

Les artefacts de déploiement (packages, scripts, fichiers de configuration) sont archivés dans un dépôt sécurisé et versionnés, permettant la reconstruction à l'identique de tout état antérieur du système. La durée de conservation minimale des archives est définie contractuellement en cohérence avec les obligations légales applicables à l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-009 : Reporting périodique sur les déploiements

Le TITULAIRE produit un rapport mensuel sur l'activité de déploiement, transmis à l'ANAH dans les cinq jours ouvrés suivant la fin de la période.

Ce rapport présente :

- Le nombre de déploiements réalisés par environnement,
- Le taux de succès des mises en production (sans rollback ni incident post-déploiement),
- Les déploiements ayant nécessité un retour arrière avec analyse des causes,
- L'état du niveau de patching du parc,
- Les déploiements planifiés pour la période suivante.

Ces indicateurs alimentent le tableau de bord qualité du marché et sont commentés lors du comité de suivi opérationnel mensuel.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-DEP-010 : Prise en charge de la chaîne CI/CD par l'infogérant et transférabilité

L'ANAH confie à l'infogérant la mise en place, l'exploitation et le maintien en condition opérationnelle de la chaîne d'intégration continue et de déploiement continu (CI/CD) utilisée pour les applications relevant du présent marché.

Le TITULAIRE est responsable :

- De la reprise, de l'adaptation, de la conception, de la mise en œuvre et de la documentation de la chaîne CI/CD,
- De la gestion des pipelines (construction, tests automatisés, contrôle qualité, déploiement sur les différents environnements),
- Du suivi et de la supervision des exécutions CI/CD,
- De la mise en place des contrôles de sécurité (gestion des secrets, contrôle des dépendances, gestion des droits, traçabilité des déploiements),
- De la formation et de l'accompagnement des équipes de l'ANAH et des éventuels tiers (équipes de développement, autres prestataires) à l'utilisation des chaînes CI/CD

La solution logicielle de CI/CD peut :

- Soit être fournie par le fournisseur de services cloud (CSP), lorsque des services managés de type CI/CD natifs du cloud sont disponibles et validés par l'ANAH,
- Soit être fournie, installée et opérée par le TITULAIRE (plateforme CI/CD dédiée ou intégrée à son outillage standard), hébergée chez le CSP et approuvée par l'ANAH.
- Le TITULAIRE étudiera les possibilités et propose une solution parmi une migration vers une nouvelle solution, la reprise de l'existant (Upgrade et gestion de bout en bout de la solution ANAH actuelle) ou une refonte complète vers une nouvelle solution SaaS.

Dans tous les cas :

- Le choix des solutions (CSP ou infogérant) est proposé par le TITULAIRE et validé par l'ANAH,
- Le TITULAIRE garantit que les solutions retenues respectent les exigences de sécurité, de conformité et de localisation des données définies par l'ANAH,
- Le TITULAIRE fournit une documentation complète (architecture, flux, configurations, scripts, procédures d'exploitation et de secours) permettant une réappropriation par l'Anah ou un tiers

Le TITULAIRE garantit la transférabilité de la chaîne CI/CD, notamment dans le cadre de la réversibilité sortante ou en cas de changement d'infogérant. À ce titre, il s'engage à :

- Éviter tout verrouillage propriétaire non justifié (technologies ou configurations non transférables sans coûts ou travaux disproportionnés),
- Structurer et maintenir les pipelines, scripts, configurations, modèles (templates) et artefacts de déploiement de manière standardisée et documentée,
- Fournir, dans le cadre de la réversibilité, l'ensemble des éléments nécessaires à la reprise de la chaîne CI/CD par l'Anah ou par un nouvel infogérant (code des pipelines, scripts d'infrastructure as code, documentation d'installation et d'exploitation, procédures de restauration),
- Accompagner, pendant la phase de réversibilité, le transfert de compétence (ateliers, sessions de présentation, support à la mise en place de la nouvelle chaîne CI/CD si nécessaire)

Les obligations détaillées du TITULAIRE en matière de transférabilité du CI/CD sont intégrées aux exigences de réversibilité du présent CCTP (réversibilité entrante et sortante).

Exigences de performance, disponibilité et sécurité. LE TITULAIRE définit et met en œuvre :

- Des engagements de disponibilité de la plateforme CI/CD et des délais de traitement des pipelines, alignés avec les besoins de l'Anah,
- Des mécanismes de sauvegarde et de reprise de la plateforme CI/CD (configuration, pipelines, référentiels d'artefacts),
- Des contrôles d'accès adaptés (séparation des rôles, gestion des comptes et droits, journalisation des actions)

Les coûts associés à la mise à disposition, à l'exploitation et à la maintenance de la chaîne CI/CD, qu'elle soit fournie par le CSP ou par le TITULAIRE, sont explicitement détaillés dans le bordereau de prix, en distinguant le cas échéant :

- Les coûts récurrents (licences, services managés CSP, exploitation, supervision),
- Les coûts de mise en place et d'évolution (création ou modification de pipelines, intégrations supplémentaires, automatisations spécifiques),
- Les coûts liés à la réversibilité de la solution CI/CD

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

g. Gestion de la continuité de service

GST-CNT-001 : Production d'un Plan de Continuité d'Activité (PCA)

Dans le cadre de la phase de réversibilité entrante, le TITULAIRE a l'obligation de disposer d'un Plan de Continuité d'Activité (PCA) couvrant l'ensemble des services relevant du présent marché, selon les modalités suivantes :

Cas d'un PCA existant

Si le TITULAIRE dispose déjà d'un PCA fourni par l'Anah couvrant tout ou partie du périmètre :

- Il procède, conjointement avec l'Anah, à son analyse et à sa mise à jour pour l'adapter aux besoins, contraintes et objectifs de continuité définis par l'Anah (processus critiques, scénarios de risque, RTO/RPO, etc.),
- Il soumet la version mise à jour à la validation de l'Anah avant la fin de la réversibilité entrante.

Cas d'absence de PCA existant

Le TITULAIRE propose et formalise un PCA spécifique à l'Anah, en s'appuyant sur les informations et priorités communiquées par l'Anah ;

- L'élaboration de ce PCA est réalisée conjointement par l'Anah et le TITULAIRE, l'Anah étant responsable de la définition et de la priorisation des besoins métier, des processus critiques, des scénarios de crise et des objectifs de continuité, et le TITULAIRE étant responsable de la proposition des mesures techniques, organisationnelles et procédurales ;
- Le TITULAIRE soumet ce PCA à la validation de l'Anah avant la fin de la phase de réversibilité entrante.

Contenu et mise à jour du PCA

Le PCA, qu'il soit issu d'une mise à jour ou d'une création, précise a minima :

- Les scénarios de crise couverts et les niveaux de service associés,
- Les modalités de bascule, de reprise et de retour à la normale,
- Les rôles et responsabilités respectifs de l'Anah et du TITULAIRE,
- Les modalités de tests de continuité (fréquence, typologie, acteurs) menés conjointement.

Le PCA est ensuite maintenu en condition opérationnelle pendant toute la durée du marché : il est revu conjointement par l'Anah et le TITULAIRE au moins une fois par an, et à chaque évolution significative du périmètre, des risques ou de l'architecture des services.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-CNT-002 : Production d'un Plan de Reprise d'Activité (PRA)

Dans le cadre de la phase de réversibilité entrante, le TITULAIRE a l'obligation de disposer d'un Plan de Reprise d'Activité (PRA) couvrant l'ensemble des services relevant du présent marché, selon les modalités suivantes :

Cas d'un PRA existant

Si le TITULAIRE dispose déjà d'un PRA fourni par l'Anah couvrant tout ou partie du périmètre :

- Il procède, conjointement avec l'Anah, à son analyse et à sa mise à jour pour l'adapter aux besoins, contraintes et objectifs de reprise définis par l'Anah (processus critiques, priorités de reprise, RTO/RPO, scénarios de sinistre, etc.),
- Il propose les mises à jour technique des procédures et des processus associés
- Il soumet la version mise à jour à la validation de l'Anah avant la fin de la phase de réversibilité entrante.

Cas d'absence de PRA existant

Le TITULAIRE propose et formalise un PRA spécifique à l'Anah, en s'appuyant sur les informations et priorités communiquées par l'Anah. L'élaboration de ce PRA est réalisée conjointement par l'Anah et le TITULAIRE, l'Anah étant responsable de la définition et de la priorisation des besoins métier, des processus critiques, des scénarios de sinistre et des objectifs de reprise (notamment RTO/RPO), et le TITULAIRE étant responsable de la proposition des mécanismes de reprise (techniques, organisationnels et procéduraux). Le TITULAIRE soumet ce PRA à la validation de l'Anah avant la fin de la phase de réversibilité entrante.

Contenu et mise en œuvre du PRA

Le PRA, qu'il soit issu d'une mise à jour ou d'une création, précise a minima :

- Les scénarios de sinistre couverts (perte de site, indisponibilité majeure, corruption de données, etc.) et les environnements concernés,
- Les architectures et moyens de reprise (sites de secours, mécanismes de sauvegarde/restauration, redondances, procédures de reconstruction),
- Les priorités de reprise par service ou composant, et les objectifs de reprise associés (RTO, RPO),
- Les procédures détaillées de bascule vers l'environnement de secours, de remise en service et de retour à la situation nominale,
- Les rôles et responsabilités respectifs de l'Anah et du TITULAIRE dans la gestion d'un sinistre majeur,
- Les modalités et la fréquence des tests de PRA (tests techniques, exercices de bascule, simulations de sinistre) menés conjointement par l'Anah et le TITULAIRE.

Maintien en condition opérationnelle

Le PRA est maintenu en condition opérationnelle pendant toute la durée du marché :

- Il est revu et actualisé conjointement par l'Anah et le TITULAIRE au moins une fois par an, ainsi qu'à chaque évolution significative du périmètre, de l'architecture, des risques ou des niveaux de service,
- Les tests de PRA sont planifiés, réalisés et formalisés selon une fréquence et des modalités validées par l'Anah,
- Les écarts constatés donnent lieu à un plan d'actions correctif suivi conjointement

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-CNT-003 : Maintien en condition opérationnelle et tests du Plan de Reprise d'Activité (PRA)

Le TITULAIRE est responsable du maintien en condition opérationnelle du Plan de Reprise d'Activité (PRA) pendant toute la durée du marché.

Le TITULAIRE met à jour le PRA à chaque évolution significative du périmètre des services, de l'architecture, des niveaux de service ou des risques identifiés. Il soumet toute version mise à jour à la validation de l'Anah, avec un tableau de suivi des modifications et s'assure de la cohérence du PRA avec le PCA et avec les SLA du marché.

Les différents scénarios de tests sont documentés, mise à jour, validés et stockés dans l'espace Confluence de l'Anah.

Tests réguliers du PRA

Le PRA fait l'objet de tests réguliers, réalisés au minimum une (1) fois par an, selon un plan de tests validé par l'Anah. Ces tests peuvent inclure, en fonction des contraintes opérationnelles :

- Des tests techniques de sauvegarde/restauration,
- Des tests de bascule partielle ou complète vers l'environnement de secours,

- Des exercices de gestion de crise et de coordination entre l'Anah et le TITULAIRE,
- Compte rendu et actions correctives

À l'issue de chaque test :

Le TITULAIRE produit un rapport de test de PRA, présentant le scénario testé, les résultats obtenus, les écarts constatés par rapport aux objectifs (RTO/RPO, niveaux de service) et les risques résiduels. Il propose, en concertation avec l'Anah, un plan d'actions correctif pour traiter les écarts et améliorer le dispositif de reprise et il met à jour le PRA le cas échéant, les procédures associées, après validation de l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

h. Gestion des sauvegardes

GST-SAUUV-001 : Besoins de sauvegarde

Le système d'information de l'Anah est hébergé dans un environnement cloud et nécessite une solution de sauvegarde complète, fiable et sécurisée.

Le TITULAIRE doit mettre en place un dispositif de sauvegarde automatisé permettant de protéger l'ensemble des données, configurations, images systèmes et composants applicatifs critiques.

Les sauvegardes doivent être réalisées selon une fréquence définie (quotidienne au minimum), avec une rétention adaptée aux exigences métiers et réglementaires, et stockées sur un support distinct de l'environnement de production (cloud tiers, datacenter distant, ou équivalent).

Le TITULAIRE doit garantir la confidentialité, l'intégrité et la traçabilité des opérations de sauvegarde et de restauration, ainsi que la résilience face aux sinistres majeurs (incident cloud, cyberattaque, erreur humaine).

Des tests réguliers de restauration doivent être effectués et documentés, afin d'assurer la disponibilité effective des données et la continuité des services du SI.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-SAUUV-002 : Méthode de sauvegarde

Les sauvegardes du SI hébergé dans le cloud sont réalisées de manière automatique au moyen des services de sauvegarde managés fournis par le prestataire cloud (par exemple, service de type Backup as Service ou équivalent pour les environnements virtualisés, et mécanismes de snapshots pour les instances et volumes).

Ces solutions permettent de réaliser des images instantanées des ressources (machines virtuelles, disques, bases de données managées, etc.) avec une fréquence au minimum quotidienne, complétée par des sauvegardes complètes hebdomadaires.

L'utilisation de ces méthodes de sauvegarde et de snapshots en ligne permet de protéger les environnements de production sans interruption de service et de garantir la préservation des systèmes dans leur intégralité (données, configurations et applications).

Les sauvegardes sont stockées sur un espace de stockage distinct et sécurisé au sein du cloud (ou sur un second cloud), afin de renforcer la résilience et de faciliter les opérations de restauration en cas d'incident.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-SAUV-003 : Contrôles de réalisation des sauvegardes

Le TITULAIRE met en œuvre un processus formalisé de vérification des sauvegardes du SI afin de garantir l'intégrité et la restaurabilité des données.

À une fréquence définie avec l'Anah, le TITULAIRE contrôle systématiquement le bon déroulement des sauvegardes (tâches planifiées, journaux d'exécution, volumes traités, alertes éventuelles, temps des sauvegardes) et consigne les résultats dans des rapports de suivi.

Le TITULAIRE réalise également des tests réguliers de validation des backups, portant sur la restauration partielle (fichiers, bases applicatives spécifiques) et la restauration complète d'environnements cibles.

Les procédures de test précisent les prérequis, les jeux de données, les étapes de restauration et les critères de succès.

Le TITULAIRE consigne les données suivantes dans des rapports de suivi de restauration.

- Type de backup : (full, snapshots, fichier, db, ...)
- Date de début
- Date de fin
- Temps de restauration
- Backup validé
- Commentaire sur le déroulement

Les écarts ou incidents constatés donnent lieu à des plans d'actions correctifs et à une mise à jour de la documentation d'exploitation et des consignes de sauvegarde / restauration.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-SAUV-004 : Protection des sauvegardes

Le TITULAIRE devra mettre en œuvre un processus de chiffrement formalisé afin de garantir la confidentialité des données sauvegardées du SI.

Toutes les sauvegardes identifiées comme sensibles sont chiffrées selon des algorithmes et des longueurs de clés conformes aux exigences de sécurité en vigueur. Le TITULAIRE s'assure de la gestion sécurisée du cycle de vie des clés (génération, stockage, rotation, révocation) et de leur séparation vis-à-vis des environnements de production.

Le TITULAIRE précise les mécanismes de chiffrement mis en œuvre (chiffrement natif du Cloud, chiffrement au niveau du système ou de l'application), ainsi que les modalités de gestion, de séparation et de rotation des clés (clés gérées par le CSP, clés client, BYOK/CMK le cas échéant).

Le TITULAIRE vérifie régulièrement l'activation effective de ces dispositifs, teste la capacité de déchiffrement lors d'exercices de restauration et consigne les résultats dans des rapports.

Tout incident ou vulnérabilité détecté entraîne des actions correctives et une mise à jour des procédures de chiffrement et d'exploitation.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

GST-SAUV-005 : Rétention des sauvegardes

Le TITULAIRE met en œuvre un processus formalisé de gestion des délais de rétention, du nombre de sauvegardes et des snapshots journaliers, afin de garantir la disponibilité des données sur la durée requise. Les périodes de conservation sont définies en accord avec les exigences métiers, contractuelles et réglementaires, et sont paramétrées dans les outils de sauvegarde pour chaque type de donnée et chaque environnement (production, préproduction, développement).

Le TITULAIRE définit et applique des politiques précises sur le nombre de copies de sauvegarde conservées (journalières, hebdomadaires, mensuelles, annuelles) ainsi que sur la réalisation de snapshots quotidiens des systèmes critiques.

Le TITULAIRE s'assure du bon déroulement des purges automatiques à l'issue des délais de rétention, afin de maîtriser la capacité de stockage et de limiter les risques de conservation excessive de données. Les paramètres de rétention, le suivi des volumes et les écarts constatés sont tracés et donnent lieu, si nécessaire, à des actions correctives et à une mise à jour de la documentation.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

i. Supervision et monitoring

SUP-MON-001 : Gestion de la Supervision et du monitoring

Le TITULAIRE devra mettre en place un dispositif de monitoring complet du Système d'Information afin de garantir la disponibilité, les performances et la sécurité des services.

Ce dispositif doit permettre une supervision en temps réel des composants techniques et applicatifs, ainsi qu'une visibilité consolidée pour l'Anah. Le monitoring vise à détecter précocement les dégradations de service, à prévenir les incidents majeurs et à faciliter les analyses post-incident.

Le TITULAIRE s'appuie sur des outils de supervision centralisés, capables de collecter, corréliser et historiser les métriques, journaux et événements issus de l'ensemble des environnements (production, préproduction, recette).

Le TITULAIRE fournit des tableaux de bord synthétiques et des rapports périodiques, permettant de suivre les niveaux de service (SLA/SLT), les tendances de charge et les risques potentiels.

Le TITULAIRE met en place une revue pour limiter les alertes fantômes.

Le dispositif de monitoring est revu régulièrement en comité de pilotage afin d'être adapté aux évolutions du SI et aux nouveaux besoins métiers.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

SUP-MON-002 : Socle de supervision

Le TITULAIRE met en place un socle de supervision couvrant à minima les éléments essentiels du SI afin d'assurer un niveau de service conforme aux engagements contractuels. À ce titre, il doit monitorer les ressources systèmes (CPU, mémoire, disque, I/O), les services et processus critiques, la disponibilité réseau (latence, pertes de paquets, bande passante), ainsi que les bases de données (espace, temps de réponse, verrous).

Les applications métiers, les serveurs applicatifs et les équipements de sécurité (firewalls, proxys, systèmes de détection d'intrusion) doivent également être intégrés au périmètre de supervision.

Le TITULAIRE s'assure par ailleurs de la supervision des sauvegardes, des tâches planifiées et des certificats (validité, expiration). La liste détaillée des éléments à monitorer, des indicateurs associés et des seuils de criticité est fournie dans une matrice de supervision, tenue à jour et validée par l'Anah.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

SUP-MON-003 : Gestion des logs

Le TITULAIRE devra mettre en place un dispositif structuré de gestion des journaux applicatifs et systèmes (logs) afin de garantir la traçabilité, la sécurité et la capacité d'audit du Système d'Information. Les logs applicatifs (transactions, erreurs fonctionnelles, authentications, appels aux services tiers) et les logs systèmes (événements systèmes, services, démarrages/arrêts, erreurs matérielles, sécurité) sont activés avec un niveau de verbosité adapté aux exigences métiers et réglementaires.

Le TITULAIRE devra centraliser, dans la mesure du possible, ces journaux au sein d'une plateforme dédiée (collecte, indexation, corrélation, recherche), permettant une consultation rapide, une analyse croisée et une conservation maîtrisée selon les politiques de rétention définies. Il met en œuvre des mécanismes d'horodatage fiable, d'intégrité des logs et de contrôle d'accès strict, afin de prévenir toute altération ou consultation non autorisée.

Les journaux sont exploités à la fois de manière réactive (diagnostic d'incident, analyse post-mortem) et proactive (détection d'anomalies, indicateurs de performance, détection de comportements suspects). Le TITULAIRE définit, documente et maintient les procédures relatives à l'activation, la rotation, l'archivage et la restauration des logs, et rend compte régulièrement à l'Anah via des rapports et tableaux de bord dédiés.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

SUP-MON-004 : Gestion des alertes

Le TITULAIRE devra mettre en œuvre des moyens d'alerting structurés afin de garantir une réactivité adaptée à la criticité des événements détectés par le monitoring. Les alertes sont générées automatiquement à partir de seuils, de corrélations d'événements et de règles de détection d'anomalies, paramétrés en concertation avec le maître d'ouvrage.

Les notifications d'alerte sont transmises via plusieurs canaux (console de supervision, e-mail, SMS, outils ITSM, messagerie collaborative) et s'appuient sur une gestion de l'astreinte et des escalades clairement définie. Chaque alerte comporte à minima le périmètre impacté, la criticité, la description de l'événement et les premières recommandations de traitement.

Le TITULAIRE devra s'assurer que les alertes sont tracées, horodatées et historisées, afin de permettre le suivi des temps de prise en charge et de résolution. Les paramètres d'alerting (seuils, canaux, niveaux de criticité) font l'objet de revues régulières pour limiter les faux positifs et garantir la pertinence opérationnelle.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.

SUP-MON-005 : Gestion des incidents et crises

En cas d'alerte majeure détectée par le dispositif de monitoring, le TITULAIRE devra appliquer sans délai un processus d'escalade et de gestion d'incident formalisé. Dès la réception de l'alerte, une qualification rapide est effectuée afin de confirmer l'impact, la criticité et le périmètre concerné. Le TITULAIRE déclenche alors la mobilisation des équipes techniques concernées et, le cas échéant, le dispositif d'astreinte.

L'Anah est informé selon les modalités définies (délai maximal, canal de communication, contenu minimal des messages). Le TITULAIRE devra mettre en œuvre les actions de contournement et de remédiation nécessaires, en documentant chaque étape.

À l'issue de l'incident, un retour d'expérience (Rex) est organisé, incluant l'analyse des causes, les actions correctives et préventives, ainsi que la mise à jour des procédures de supervision, d'alerting et d'exploitation pour limiter la récurrence.

Voir les exigences de gestion des incidents et des problèmes qui viennent compléter celle-ci.

Niveau à atteindre (Les pénalités si applicables sont décrites dans la CCAP) :

Respect de l'exigence tout au long du marché.