PREMIER MINISTRE
*Liberté*
*Égalité*
*Fraternité*

**Secrétariat général du Gouvernement**

Direction des services
administratifs et financiers

**Cahier des Clauses Techniques Particulières (CCTP) relatif à la :**

« Tierce maintenance applicatives des applications informatiques et sites web des services du Premier ministre »

# Table des matières


TERMINOLOGIES ..... 5

**ARTICLE 1 - CONTEXTE ET OBJET DE L'ACCORD-CADRE ..... 6**

1.1. CONTEXTE DE L'ACCORD-CADRE ..... 6
*1.1.1 Présentation de la DSI/DSAF ..... 6*
*1.1.2. Présentation des entités administratives ..... 7*
*1.1.3. Contexte technique général ..... 7*
*1.1.4. Contexte sécurité ..... 8*
1.2. OBJET DE L'ACCORD-CADRE ..... 8
*1.2.1 Structure de l'accord-cadre ..... 8*

**ARTICLE 2 - DISPOSITIONS COMMUNES AUX LOTS ..... 10**

2.1. ACCESSIBILITE NUMERIQUE ..... 11
2.2. DOCUMENTS DE REFERENCE ET APPLICABLES ..... 11
2.3. DESCRIPTIONS DES PRESTATIONS ATTENDUES ..... 12
*2.3.1. Attentes générales liées aux prestations ..... 12*
2.4. PILOTAGE ET COORDINATION DE LA PRESTATION ..... 12
2.5. MAINTENANCE CORRECTIVE (MC) ..... 12
*2.5.1. Définition ..... 12*
*2.5.2. Prestations attendues ..... 13*
*2.5.3. Niveau de criticité d'une anomalie ..... 13*
*2.5.4. Documentation ..... 14*
2.6. NIVEAUX DE COMPLEXITE ..... 14
*2.6.1. Niveau de complexité technique et fonctionnelle ..... 14*
*2.6.2. Niveau de complexité globale ..... 15*
2.7. MAINTENANCE CORRECTIVE TRIMESTRIELLE (MC) ..... 16
*2.7.1. Exigences de sécurité ..... 16*
*2.7.2. Maintenance préventive trimestrielle ..... 17*
2.8. SUPPORT ..... 17
2.9. CONSEIL ET EXPERTISE ..... 17
2.10. QUALITE ET SECURITE DES DEVELOPPEMENTS ..... 18
2.11. ACCES AUX ENVIRONNEMENTS ..... 18

**ARTICLE 3 - PRESTATION D'INITIALISATION (POSTE N°1) ..... 19**

3.1. INITIALISATION DE LA MAINTENANCE ET PRESTATIONS DU PERIMETRE INITIAL (UO1) ..... 19
*3.1.1. Description de la phase d'initialisation ..... 19*
*3.1.2. Périmètre initial ..... 21*
3.1.2.1. Applications dites « standards » (lot 1) ..... 21
3.1.2.2. Applications basées sur les technologies ALFRESCO & NUXEO (lot 2) ..... 21
3.1.2.3. Sites internet & intranet (lot 3) ..... 21
3.1.2.4. Applications basées sur la technologie ODOO (lot 4) ..... 22

**ARTICLE 4 - PRESTATIONS DU SOCLE : MAINTENANCE CORRECTIVE ET PREVENTIVE (POSTE N°2 - VOLET 1) ..... 22**

4.1. DESCRIPTION DES PRESTATIONS ..... 22
4.2. DIMENSIONNEMENT DU POSTE – MAINTENANCE CORRECTIVE TRIMESTRIELLE (UO2) ..... 22
4.3. DIMENSIONNEMENT DU POSTE – MAINTENANCE PREVENTIVE (UO3) ..... 23
4.4. ORGANISATION DES RESSOURCES ..... 23

**ARTICLE 5 - PRESTATIONS HORS SOCLE (POSTE 3 ET POSTE 4 - VOLET 2) ..... 23**

5.1. MAINTENANCE CORRECTIVE ET PREVENTIVE TRIMESTRIELLE HORS SOCLE (UO4 A UO6) ..... 23
5.1.1. Définition du périmètre hors socle ..... 23

**5.2. Résolution des anomalies (poste 4 : UO7 à UO15)** ... 24

**ARTICLE 6 - MAINTENANCE EVOLUTIVE (POSTE 5 : UO16 A UO18)** ... **24**

*6.1. Définition* ... *24*
*6.2. Nature des prestations* ... *25*
*6.3. Processus de mise en œuvre* ... *25*
*6.4. Réalisation des prestations* ... *25*
*6.5. Recette et validation* ... *25*
*6.6. Modalités de calcul* ... *25*
*6.7. Livrables UO16 à UO18* ... *26*

**ARTICLE 7 - ÉTUDE D'IMPACT OU D'ANALYSE (POSTE 6 : UO19 A UO20)** ... **26**

*7.1. Objet* ... *26*
*7.2. Typologie* ... *27*
*7.3. Modalités* ... *27*
*7.4. Livrables attendus UO19 à UO20* ... *27*

**ARTICLE 8 - ENTREE D'UN NOUVEAU SITE WEB OU D'UNE APPLICATION DANS LE PERIMETRE (POSTE 7 : UO21 A UO23)** ... **27**

*8.1. Objet* ... *27*
*8.2. Phase préalable* ... *28*
*8.3. Prise en charge* ... *28*
*8.4. Livrables attendus UO21 à UO23* ... *28*

**ARTICLE 9 - PRESTATIONS PONCTUELLES DE TMA HORS PERIMETRE (POSTE 8 : UO24 A UO26)** **28**

*9.1. Objet* ... *28*
*9.2. Modalités* ... *28*
*9.3. Livrables attendus UO24 à UO26* ... *28*

**ARTICLE 10 - REVERSIBILITE (POSTE 9 : UO27 A UO30)** ... **29**

*10.1. Objet* ... *29*
*10.2. Types* ... *29*
*10.3. Contenu* ... *29*
*10.4. Délais* ... *29*
*10.5. Livrables attendus UO27 à UO30* ... *29*

**ARTICLE 11 - EXIGENCES ET ENGAGEMENTS** ... **29**

11.1. EXIGENCES DE SECURITE ... 29
11.1.1. CONFORMITE A L'ETAT DE L'ART ... 29
11.1.2. GESTION DES BIENS ET DES DONNEES ... 30
11.1.3. SECURITE DU POSTE DE TRAVAIL ... 31
11.1.4. CONFORMITE, AUDIT ET CONTROLE ... 31
11.2. EXIGENCES LIEES AUX PRESTATIONS D'ETUDE ... 31
11.3. EXIGENCES LIEES AUX DEVELOPPEMENTS ... 31
11.3.1. INVENTAIRE DES COMPOSANTS ... 32
11.4. EXIGENCES RELATIVES AU PERSONNEL ... 33
*11.4.1. Qualifications et expérience* ... *33*
*11.4.2. Gestion des ressources* ... *33*
11.5. CONVENTION DE NIVEAU DE SERVICE (CNS) ... 33
*11.5.1. Définition des sévérités* ... *33*
*11.5.2. Délais de traitement* ... *34*
*11.5.3. Niveaux de service attendus* ... *34*
*11.5.4. Mesure des délais* ... *34*
*11.5.5. Interventions hors horaires* ... *34*

11.6. LIVRAISON ET VALIDATION DES DOCUMENTS ..... 35
*11.6.1. Modalités de livraison* ..... *35*
*11.6.2. Validation* ..... *35*
11.7. LIVRAISON DES COMPOSANTS LOGICIELS ..... 35
*11.7.1. Mise en production* ..... *35*
*11.7.2. Validation de sécurité* ..... *35*
11.8. GESTION DES DEMANDES ET INCIDENTS ..... 36
*11.8.1. Outil de gestion des tickets* ..... *36*
*11.8.2. Qualification des anomalies* ..... *36*
*11.8.3. Cycle de vie des incidents* ..... *36*

**ARTICLE 12 - ORGANISATION ET RESPONSABILITES ..... 36**

12.1. LES ROLES ET RESPONSABILITES ..... 36
*12.1.1. L'entité des SPM responsable du site web ou de l'application* ..... *36*
*12.1.2. La DSI/DSAF - Responsable contractuel* ..... *37*
*12.1.3. Répartition des rôles* ..... *37*
12.2. GOUVERNANCE ET PILOTAGE ..... 38
*12.2.1. Le Comité de suivi (COSUI)* ..... *38*
*12.2.2. Le Comité de Pilotage (COPIL)* ..... *39*

**ARTICLE 13 - PLAN QUALITE DU PROJET ET DES PRESTATIONS ..... 40**

13.1. PLAN D'ASSURANCE QUALITE (PAQ) ..... 40
13.2. SUIVI DE LA QUALITE DES PRESTATIONS ..... 41

**ARTICLE 14 - ANNEXES ..... 41**

14.1. POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DE L'ÉTAT (PSSIE) ..... 41
14.2. VOLET INITIAL : LISTE DU PARC APPLICATIF INITIAL DE L'ACCORD-CADRE TMA DES SITES INTERNET ET APPLICATIONS ..... 41
14.3. LE CADRE DE COHERENCE TECHNIQUE ..... 41
14.4. LA MATRICE DE COMPLEXITE ..... 41

## TERMINOLOGIES

| Terme | Signification |
|---|---|
| AAI | Autorité administrative indépendante |
| ANSSI | Agence nationale de la sécurité des systèmes d'information |
| AMOE | Assistance au maître d'œuvre |
| ARDP | Autorité de régulation de la distribution de la presse |
| CCAP | Cahier des clauses administratives particulières |
| CCNE | Comité consultatif national d'éthique |
| CCTP | Cahier des clauses techniques particulières |
| CIVS | Commission pour l'indemnisation des victimes de spoliations |
| CNCDH | Commission nationale consultative des droits de l'homme |
| COMOP | Comité opérationnel |
| COPIL | Comité de pilotage |
| COSUI | Comité de suivi |
| CSR | Comité de suivi des retraites |
| DCT | Document de conception technique |
| DDD | Défenseur des Droits |
| DEX | Dossier d'exploitation |
| DIN | Dossier d'installation |
| DSAF | Direction des services administratifs et financiers |
| DSI/DSAF | Division des systèmes d'information |
| DTV | Dossier de Tests de Validation (intégrant le cahier de tests) |
| MCO | Maintien en condition opérationnelle |
| MCS | Maintien en condition de sécurité |
| MI | Ministère de l'Intérieur |
| MILDECA | Mission interministérielle de lutte contre les drogues et les conduites addictives |
| PAQ | Plan d'assurance qualité |
| RIE | Réseau interministériel de l'État |
| SFD | Spécifications fonctionnelles détaillées |
| SI | Système d'information |
| SIG | Service d'information du gouvernement |
| SPM | Services du Premier ministre |
| SSI | Sécurité des systèmes d'information |
| TMA | Tierce maintenance applicative |
| VA | Vérification d'aptitude |
| Volet 1 | Prestations dites « socle » |
| Volet 2 | Prestations dites « hors socle » |
| VSR | Vérification de service régulier |
| UO | Unité d'œuvre |

## Article 1 - Contexte et Objet de l'accord-cadre

### 1.1. Contexte de l'accord-cadre

La Direction des Systèmes d'Information (DSI) de la Direction des Services Administratifs et Financiers (DSAF) assure le soutien informatique d'un ensemble d'entités administratives, majoritairement rattachées aux Services du Premier Ministre (SPM).

Le périmètre des entités soutenues est susceptible d'évoluer en fonction des évolutions organisationnelles.

La DSI/DSAF est responsable du pilotage du présent accord-cadre et de la bonne exécution des prestations réalisées par le titulaire.

La réalisation des prestations repose sur une collaboration étroite entre :

- la DSI/DSAF,
- les entités bénéficiaires,
- le titulaire de l'accord-cadre.

Le périmètre initial de l'accord-cadre porte sur des applications faisant déjà l'objet de prestations de tierce maintenance applicative.

Des applications et des sites intranet/internet supplémentaires peuvent être intégrés à l'accord-cadre via le volet à bons de commande.

Des applications et des sites intranet/internet peuvent par ailleurs être en fin de cycle de vie et faire l'objet d'opérations de refonte ou d'arrêt.

#### 1.1.1 Présentation de la DSI/DSAF

La DSI est structurée autour de cinq entités :

- **Le bureau de l'intégration et des opérations (BIO)**, chargé :
    - de l'exploitation et de l'administration du système d'information (systèmes, réseaux et applications) ;
- **Le bureau des études et des projets numériques (BEPN)**, chargé :
    - des projets et produits métiers ainsi que des études ;
    - du maintien en condition opérationnelle et de sécurité des applicatifs ;
- **Le pôle Architecture et SSI (PASSI)**, chargé :
    - de l'architecture du système d'information ;
    - de la sécurité des systèmes d'information (SSI) ;
- **La cellule d'organisation et de pilotage de l'activité (COPA)**, chargée :
    - du suivi et de l'organisation de l'activité ;
    - du budget et des achats ;
- **Le bureau du support informatique et des télécommunications (BSIT)**, chargé :
    - du support de proximité et du support de premier niveau ;

- de la téléphonie ;
- de l'architecture technique.

La DSI soutient environ 2 500 utilisateurs, avec un niveau d'intégration variable au sein du système d'information.

Elle assure l'hébergement, l'exploitation et la gestion de son système d'information, tout en ayant recours, pour certaines applications, à des solutions d'hébergement externalisées ou mutualisées.

La DSI :

- s'assure de la bonne exécution contractuelle de l'accord-cadre ;
- accompagne les entités administratives dans la mise en œuvre des processus et méthodologies ;
- organise la coordination entre les différentes parties prenantes.

### 1.1.2. Présentation des entités administratives

Il existe deux catégories d'entités :

- **Les entités administratives rattachées au périmètre budgétaire des SPM**, qui participent à l'élaboration de la politique gouvernementale ;
- **Les autorités administratives indépendantes (AAI)**, qui assurent des missions de régulation sans lien hiérarchique avec un ministre.

Les entités rattachées au périmètre budgétaire des SPM bénéficient de l'ensemble des prestations de l'accord-cadre, sous pilotage de la DSI/DSAF.

Les AAI peuvent également bénéficier des prestations, avec un pilotage propre, assisté par la DSI/DSAF sur les aspects contractuels.

### 1.1.3. Contexte technique général

➢ Aspect technologique :

Le périmètre applicatif et les socles techniques associés sont décrits en annexe.

➢ Aspects hébergement et exploitation :

La DSI/DSAF opère son propre système d'information.

Les applications sont hébergées et exploitées selon les modalités suivantes :

- au sein des systèmes d'informations internes de la DSI/DSAF ;
- auprès d'un prestataire d'hébergement externe ;
- au sein d'un hébergement étatique mutualisé.

Les opérations d'exploitation sont réalisées par les équipes compétentes selon les modalités définies dans le plan d'assurance qualité (PAQ).

Aucune action d'administration à distance, notamment via une connexion VPN, n'est autorisée pour le titulaire.

Les réseaux sont segmentés et les flux applicatifs transitent via des dispositifs de filtrage.

Les environnements techniques reposent notamment sur :

- Debian (versions supportées) ;
- PostgreSQL (versions supportées) ;

Dans le cas d'hébergements externes, les choix techniques sont définis avec les prestataires concernés.

Les exigences de sécurité sont conformes aux cadres réglementaires obligatoires comme le Référentiel Général de Sécurité (RGS), à la Politique de Sécurité des SI de l'Etat (PSSIE), à la directive NIS/NIS2, à la protection des informations sensibles (IGI/DR/secret) et aux référentiels et cadres opérationnels de l'ANSSI (homologation de sécurité, méthode EBIOS Risk Manager et référentiel cyber national).

Des évolutions des modalités d'hébergement peuvent intervenir en cours d'exécution de l'accord-cadre. Le titulaire s'y adapte.

#### 1.1.4. Contexte sécurité

La sécurité constitue une exigence majeure du présent accord-cadre.

Le titulaire se conforme aux exigences de sécurité définies par les SPM ainsi qu'aux référentiels de l'ANSSI et, à leurs évolutions.

Les exigences décrites au présent CCTP constituent un socle minimal. Le titulaire demeure responsable de la mise en œuvre des mesures de sécurité adaptées, conformément à l'état de l'art.

### 1.2. Objet de l'accord-cadre

Le présent accord-cadre a pour objet la tierce maintenance applicative (TMA) des applications informatiques et des sites web des services du Premier ministre.

Les applications désignent un programme disponible sur un serveur à distance et qui réalise des fonctions spécifiques pour son utilisateur. Elles permettent aux utilisateurs de gérer des travaux et des documents grâce à leur capacité à fonctionner sur tous les types de navigateurs.

Les sites web sont caractérisés par une fonction unique de consultation d'informations à partir d'une interface graphique, à la différence d'applications web ayant pour objectif de réaliser des tâches spécifiques (exemple : achat de produits, jeux en ligne, etc.).

#### 1.2.1 Structure de l'accord-cadre

L'accord-cadre est décomposé en **quatre lots distincts**, correspondant à des périmètres techniques spécifiques en matière de tierce maintenance.

Cet allotissement vise à assurer une adéquation entre les compétences attendues des titulaires et les caractéristiques des systèmes concernés.

- **Lot n°1 : Tierce maintenance applicative des applications dites « standards »**

Le lot n°1 a pour objet la réalisation de prestations de tierce maintenance applicative portant sur un ensemble d'applications dites « standards » du système d'information.

Ces applications reposent sur des technologies variées et nécessitent des prestations comprenant notamment :

- la maintenance corrective ;
- la maintenance évolutive ;
- le maintien en condition de sécurité logicielle et la maintenance préventive ;
- l'assistance technique et fonctionnelle ;
- l'optimisation technique et fonctionnelle des applications

➢ **Lot n°2 : Tierce maintenance applicative des applications basées sur les technologies ALFRESCO et NUXEO**

Le lot n°2 concerne la tierce maintenance applicative d'applications reposant sur des solutions de gestion de contenu d'entreprise, notamment Alfresco et Nuxeo.

En raison des spécificités de ces technologies, ce lot requiert des compétences techniques spécialisées.

Les prestations attendues incluent notamment :

- la maintenance corrective ;
- la maintenance évolutive ;
- le maintien en condition de sécurité logicielle et la maintenance préventive ;
- l'administration technique des plateformes ;
- la gestion des évolutions et des montées de version ;
- l'optimisation technique et fonctionnelle des applications ;
- l'intégration avec les autres composants du système d'information.

➢ **Lot n°3 : Tierce maintenance des sites web**

Le lot n°3 porte sur la maintenance des sites web institutionnels, applicatifs et intranet.

Les prestations comprennent notamment :

- la maintenance corrective ;
- la maintenance évolutive ;
- le maintien en condition de sécurité des sites et la maintenance préventive ;
- l'optimisation technique et fonctionnelle des sites ;
- l'intégration de nouveaux services et fonctionnalités.

- **Lot n°4 : Tierce maintenance applicative des applications basées sur la technologie ODOO**

Le lot n°4 concerne la tierce maintenance applicative d'applications reposant sur la technologie ODOO.

En raison des spécificités de ces technologies, ce lot requiert des compétences techniques spécialisées.

Les prestations attendues incluent notamment :

- la maintenance corrective ;
- la maintenance évolutive ;
- le maintien en condition de sécurité logicielle et la maintenance préventive ;
- l'administration technique des plateformes ;
- la gestion des évolutions et des montées de version ;
- l'optimisation technique et fonctionnelle des applications ;
- l'intégration avec les autres composants du système d'information.

| Lot | Intitulé | Description / périmètre | Spécificités |
|---|---|---|---|
| **Lot n°1** | Tierce maintenance applicative des applications dites « standards » | Réalisation de prestations de tierce maintenance applicative portant sur un ensemble d'applications dites « standards » du système d'information. | — |
| **Lot n°2** | Tierce maintenance applicative des applications basées sur les technologies ALFRESCO et NUXEO | Tierce maintenance applicative d'applications reposant sur des solutions de gestion de contenu d'entreprise, notamment Alfresco et Nuxeo. | En raison des spécificités de ces technologies, ce lot requiert des compétences techniques spécialisées. |
| **Lot n°3** | Tierce maintenance des sites web | Maintenance des sites web institutionnels, applicatifs et intranet. | — |
| **Lot n°4** | Tierce maintenance applicative des applications basées sur la technologie ODOO | Tierce maintenance applicative d'applications reposant sur la technologie Odoo. | En raison des spécificités de cette technologie, ce lot requiert des compétences techniques spécialisées. |

## Article 2 - Dispositions communes aux lots

Chaque lot donne lieu à une exécution et un pilotage spécifique, conformément aux dispositions définies dans le présent CCTP.

L'accord-cadre est structuré en deux volets :

- **Volet 1 – Prestations (« socle »)** :
    - **INIT** : phase d'initialisation et de prise en charge du périmètre initial ;

- **TMA** : phase couvrant la maintenance corrective, ainsi que le maintien en condition opérationnelle et de sécurité des applications du périmètre initial.

- **Volet 2 – Prestations (« hors socle »)** :
  - réalisation d'évolutions fonctionnelles ;
  - intégration de nouvelles applications dans le périmètre de la TMA ;
  - réalisation d'études ;
  - prestations ponctuelles de maintenance ou d'assistance ;
  - opérations de réversibilité.

Dans ce document et afin d'éviter toute confusion, il est précisé les correspondances suivantes :

- **Volet 1** : Prestations dites « socle » du présent accord-cadre.
- **Volet 2** : Prestations dites « hors socle » du présent accord-cadre.
- **Titulaire** : Le « prestataire titulaire » du présent accord-cadre.
- **Prestataire** : Tout autre prestataire que le titulaire du présent accord-cadre, tel que :
  - les prestataires tiers,
  - les prestataires sortants,
  - les prestataires d'une refonte,
  - les prestataires successeurs du titulaire.

### 2.1. Accessibilité numérique

Les services numériques de l'État, et donc ceux des SPM, sont soumis à l'obligation d'accessibilité, mesurée par leur conformité au Référentiel Général d'Amélioration de l'Accessibilité (RGAA). Cette obligation concerne les services externes, sites internet pour les citoyens, comme ceux mis à la disposition des agents des SPM, sites et applications intranet. Des contrôles peuvent être réalisés par l'ARCOM.

Dans un premier temps, le niveau d'accessibilité des différents services numériques doit être maintenu.
La DSI peut procéder à des audits des applications pour établir le niveau d'accessibilité. En fonction des résultats, elle peut passer une commande d'évolution afin d'élever le niveau d'accessibilité des applications. Dans le cadre de ces travaux, la DSI peut demander d'intégrer le Design système de l'Etat (DSFR) dans les applications.

Par la suite, lors de chacune des évolutions, le titulaire veille à garantir le niveau d'accessibilité des applications sans coûts supplémentaires (à référentiel RGAA constant). Toute baisse du niveau d'accessibilité est prise en compte à la charge du titulaire dans le cadre de la TMA, sans coûts supplémentaires.

En outre, le titulaire désigne en début d'accord-cadre son référent accessibilité. Il veille notamment à la formation des équipes de développement et de design du titulaire en matière d'accessibilité.

### 2.2. Documents de référence et applicables

Les documents de référence, dans leur version en vigueur, applicables au présent accord-cadre sont :

- PSSI-E (Politique de sécurité des systèmes d'information de l'État) ;
- RGS (Référentiel Général de Sécurité) ;
- RGAA (Référentiel Général d'Accessibilité des Administrations) ;
- RGI (Référentiel Général d'Interopérabilité) ; RGPD.

## 2.3. Descriptions des prestations attendues

### 2.3.1. Attentes générales liées aux prestations

Les prestations attendues dans le cadre du présent accord-cadre doivent garantir un niveau de qualité élevée.

À ce titre, le titulaire doit notamment assurer :

- la gestion et le suivi de la qualité des prestations de maintenance corrective, évolutive et le maintien en condition de sécurité, en s'appuyant le cas échéant sur des référentiels reconnus (ISO, RGAA, ITIL ou équivalent) ;
- la mise en œuvre de dispositifs de tests techniques et de non-régression avant toute livraison ;
- le maintien d'un niveau de compétence technique adapté aux applications et sites intranet/internet du périmètre, notamment pour la sécurité SI et l'accessibilité numérique ;
- la maîtrise des activités de gestion de projet (planification, suivi des livrables, respect des délais et des engagements contractuels).

Le titulaire définit, pour chaque type de prestation, les ressources mobilisées ainsi que les délais de prise en compte et de réalisation, en fonction de la criticité.

## 2.4. Pilotage et coordination de la prestation

Le pilotage a notamment pour objectifs la maîtrise des demandes, la continuité de service, la maîtrise des coûts, des délais et des ressources, le suivi de la performance, l'adaptation aux variations de charge et la pérennisation des connaissances.

À ce titre, le titulaire assure notamment :

- l'organisation et la participation aux instances de gouvernance (cf. article 12), incluant la préparation des supports, ordres du jour et comptes rendus ;
- la production de rapports d'activité ;
- la mise en œuvre et l'exploitation d'un outil de gestion et de suivi des demandes ;
- le suivi des indicateurs de performance définis dans le PAQ ;
- la mise à jour des documents contractuels, dont le PAQ ;
- le traitement des expressions de besoins ;
- toute action nécessaire au bon déroulement des prestations.

## 2.5. Maintenance corrective (mc)

### 2.5.1. Définition

La maintenance corrective a pour objet de corriger les anomalies affectant le fonctionnement des applications.

Elle vise à garantir la continuité de service, à maintenir un niveau de qualité satisfaisant et à assurer un support technico-fonctionnel aux utilisateurs.

### 2.5.2. Prestations attendues

Le titulaire doit notamment :

- assurer la prise en charge et le traitement des anomalies ;
- réaliser le diagnostic des incidents selon un modèle transmis par la DSAF/DSI ;
- proposer et mettre en œuvre les corrections ;
- respecter les délais associés aux niveaux de criticité ;
- assurer la traçabilité des interventions ;
- réaliser les tests unitaires, d'intégration et de non-régression avec fourniture du rapport de tests à la DSAF/DSI ;
- être en capacité de réaliser des tests de performance en particulier sur les composants critiques avec fourniture du rapport de tests à la DSAF/DSI ;
- réaliser des tests d'analyse du code avec des outils de référence selon l'environnement technique afin de garantir la qualité et la sécurité du code ;
- vérifier la présence de vulnérabilités et fournir un rapport de sécurité à la DSAF/DSI à chaque livraison ;
- produire les livrables associés (documentation, rapports de tests et de sécurité, suivi des anomalies) ;
- mettre à jour la documentation technique et d'exploitation (à minima DCT, DIN, DEX) ;
- livrer les correctifs selon les exigences de l'article 11.7 « Livraison des composants logiciels » ;
- tenir à jour et transmettre à la DSAF/DSI des tableaux de bord mensuel de suivi des incidents.

### 2.5.3. Niveau de criticité d'une anomalie

Les anomalies sont classées selon trois niveaux :

- **Bloquante** : empêche l'utilisation de fonctionnalités essentielles et/ou les travaux en cours, sans solution de contournement ;
- **Majeure** : dégrade fortement le service et/ou les travaux en cours, avec solution de contournement ;
- **Mineure** : n'impacte pas significativement l'usage et/ou les travaux en cours.

La qualification est réalisée par la DSI/DSAF en lien avec le métier. En cas de désaccord, cette dernière a la décision finale.

Le titulaire est responsable du diagnostic et de la résolution.

### 2.5.4. Documentation

Toute anomalie liée à la documentation est traitée comme une anomalie corrective. Cela couvre toute incohérence, erreur, contradiction, omission, ambiguïté, non-conformité ou manque dans la documentation fournie à la DSI/DSAF.

La documentation couvre le fonctionnement des principales briques du code, et tous les éléments décrivant l'architecture, le déploiement, l'exploitation des briques de l'application.

## 2.6. Niveaux de complexité

### 2.6.1. Niveau de complexité technique et fonctionnelle

Le niveau de complexité technique & fonctionnelle des applications et sites intranet/internet est déterminé selon la matrice suivante :
Cette matrice, ses critères et ses échelles de notation présentent un caractère intangible pendant toute la durée de l'accord-cadre.

| | Critère | Description | Échelle (1-3) |
|---|---|---|---|
| **ARCHITECTURE** | **Technologies utilisées** | Nombre et diversité (langages, frameworks, bases de données, middleware). | 1 = Simple (1-2 technologies)<br>2 = Modéré (3-4 technologies)<br>3 = Complexe (>4 technologies ou obsolètes) |
| | **Infrastructure** | Type d'hébergement (on-premise, cloud, multi-cloud, conteneurisation). | 1 = Simple (on-premise)<br>2 = Modéré (cloud public)<br>3 = Complexe (multi-cloud + Kubernetes) |
| | **Sécurité** | Niveau de sensibilité (RGPD, secret défense, PSSI, chiffrement, IAM) | 1 = Standard<br>2 = Renforcé<br>3 = Très sensible (ex : ANSSI). |
| **MAINTENANCE** | **Maturité du code** | Ancienneté, dette technique, documentation | 1 = Récente (<5 ans)<br>2 = Moyenne (5-10 ans)<br>3 = Ancienne (>10 ans ou dette technique élevée). |
| | **Volume de données** | Taille des bases, flux de données | 1 = Faible (<100 Go)<br>2 = Modéré (100 Go - 1 To)<br>3 = Élevé (>1 To ou temps réel) |

| ARCHITECTURE | Critère | Description | Échelle (1-3) |
|---|---|---|---|
| | **Mise à jour** | Fréquence des releases et patches de sécurité | 1 = Rare (<1/an)<br>2 = Régulière (mensuelle)<br>3 = Fréquente (hebdomadaire ou continue) |
| | **Compatibilité** | Besoin de maintenir des versions legacy | 1 = Aucune<br>2 = Modéré (1-2 versions legacy<br>3 = Complexe (multi-versions ou très anciennes) |
| **IMPACT MÉTIER** | **Criticité métier** | Impact d'une indisponibilité | 1 = Faible (interne)<br>2 = Modéré (public)<br>3 = Élevé (vital) |
| | **Nombre d'utilisateurs** | Utilisateurs internes vs grand public | 1 = Faible (<1 000)<br>2 = Modéré (1 000 - 100 000)<br>3 = Élevé (>100 000) |
| | **Haute disponibilité** | Exigences de SLA | 1 = Faible (<99%)<br>2 = Modéré (99-99,9%)<br>3 = Élevé (>99,99%) |

### 2.6.2. Niveau de complexité globale

Trois niveaux de complexité globale sont définis :

- **Simple : note strictement inférieure à 1,67**
- **Moyenne : note supérieure ou égale à 1,67 et strictement inférieure à 2,33**
- **Complexe : note supérieure ou égale à 2,33**

| Applications / Intranet / Sites internet | A. ARCHITECTURE | | | | B. MAINTENANCE | | | | | C. IMPACT METIER | | | | Complexité globale (A+B+C)/3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1. Technologies | 2. Infrastructure | 3. Sécurité | A. Moyenne (1+2+3)/3 | 4. Maturité du code | 5. Volume de données | 6. Mise à jour | 7. Compatibilité | B. Moyenne (4+5+6+7)/4 | 8. Criticité métier | 9. Nombre d'utilisateurs | 10. Haute disponibilité | C. Moyenne (8+9+10)/3 | |
| Nom applications | 1 à 3 | 1 à 3 | 1 à 3 | | 1 à 3 | 1 à 3 | 1 à 3 | 1 à 3 | | 1 à 3 | 1 à 3 | 1 à 3 | | Note moyenne obtenue |

| Applications / Intranet / Sites internet | A. ARCHITECTURE | | | | B. MAINTENANCE | | | | | C. IMPACT METIER | | | | Complexité globale (A+B+C)/3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nom intranet | 1 à 3 | 1 à 3 | 1 à 3 | | 1 à 3 | 1 à 3 | 1 à 3 | 1 à 3 | | 1 à 3 | 1 à 3 | 1 à 3 | | Note moyenne obtenue |
| Nom sites | 1 à 3 | 1 à 3 | 1 à 3 | | 1 à 3 | 1 à 3 | 1 à 3 | 1 à 3 | | 1 à 3 | 1 à 3 | 1 à 3 | | Note moyenne obtenue |

Les critères de la matrice figurant à l'article 2.6.1, leurs échelles de notation et les seuils de complexité globale définis au présent article ne peuvent être ni modifiés, ni complétés, ni pondérés différemment à l'initiative du titulaire. Ils ne sont pas affectés par les évolutions technologiques ou organisationnelles intervenant en cours d'exécution. Toute modification de la matrice, des échelles ou des seuils ne peut intervenir que par avenant, dans les conditions de la clause de réexamen du CCAP.

La notation de chacun des critères, le calcul des moyennes par domaine et la détermination du niveau de complexité globale relèvent de la seule DSI/DSAF, qui les arrête unilatéralement. Le titulaire ne peut subordonner l'exécution d'une prestation à la révision de la notation retenue, ni en faire un motif de refus, de suspension ou de majoration, ni rattacher la prestation à une unité d'œuvre autre que celle correspondant au niveau de complexité ainsi déterminé.

La notation de chaque application, intranet et site internet est arrêtée par la DSI/DSAF lors de la phase d'initialisation pour le périmètre initial et, pour toute application ou tout site entrant ultérieurement, lors de son entrée dans le périmètre. Elle est communiquée au titulaire et consignée au compte rendu du comité de suivi. Le titulaire peut présenter des observations écrites dans un délai de **cinq (5) jours ouvrés** à compter de cette communication ; ces observations ne sont pas suspensives et la DSI/DSAF statue définitivement.

La DSI/DSAF peut, de sa seule initiative, réexaminer la notation d'une application ou d'un site lorsqu'un changement affectant l'un des critères le justifie, notamment une montée de version majeure, un changement d'hébergement, une évolution du volume de données ou du niveau d'exigence de disponibilité. La notation révisée est communiquée au titulaire et s'applique aux prestations commandées postérieurement à cette communication, sans effet sur les bons de commande en cours d'exécution.

## 2.7. Maintenance corrective trimestrielle (MC)

### 2.7.1. Exigences de sécurité

Le titulaire participe aux démarches de sécurité, notamment aux analyses de risques, aux audits de sécurité et aux opérations d'homologation ou de réhomologation.

Lorsque des composants logiciels ou la configuration des produits dont il a la responsabilité font l'objet de vulnérabilités, il fournit les éléments techniques nécessaires à l'appréciation du risque et corrige les vulnérabilités.

Les vulnérabilités sont classées selon trois niveaux dont l'importance est illustrée par le score CVSS v3.1 (ou v4.0 pour les nouvelles vulnérabilités) ou l'évaluation de l'ANSSI :

- **Critique/Elevée** : correctif urgent avec un délai maximal de 72 heures ouvrées ;
- **Moyenne** : correctif avec un délai maximal de **cinq (5) jours ouvrés** ;
- **Mineure** : évaluation au cas par cas

Le titulaire concourt à la qualification de la vulnérabilité avec la DSI/DSAF. Le pouvoir adjudicateur conserve le choix définitif du niveau retenu.

Le titulaire est responsable du diagnostic et de la résolution.

#### 2.7.2. Maintenance préventive trimestrielle

La maintenance préventive vise à prévenir les anomalies et/ou l'obsolescence et maintenir la sécurité des applications et des sites intranet/internet.

Le titulaire s'engage à assurer :

- la veille technologique ;
- le suivi et la mise en œuvre des mises à jour de sécurité ;
- l'analyse et le traitement des obsolescences ;
- la réalisation d'inventaires techniques ;
- la production de rapports :
    - d'analyse de sécurité de code (type Checkmarx ou équivalent) à chaque livraison majeure, et à la demande motivée de la DSAF/DSI
    - d'analyse des vulnérabilités des dépendances logicielles (type Dependency-Track ou équivalent) mensuelles, à chaque livraison majeure, ou à la demande motivée de la DSAF/DSI

Le titulaire propose et met en œuvre les mises à jour nécessaires dans l'objectif de conserver une solution logicielle ne présentant pas de vulnérabilités connues et exploitables. A minima, une livraison complète est produite tous les deux mois.

D'autres types de rapports visant à assurer le maintien en conditions de sécurité peuvent être demandés par la DSAF/DSI au cours de l'accord-cadre en fonction des évolutions réglementaires et des préconisations de l'ANSSI.

### 2.8. Support

Le titulaire assure un support technique de niveau 2 et un support fonctionnel de niveau 3.

Les demandes sont traitées dans le cadre de la maintenance corrective.

Le titulaire intervient notamment lors des phases de qualification, lors des mises en production et en assistance à l'exploitation.

### 2.9. Conseil et expertise

Le titulaire réalise des prestations de conseil et d'expertise portant notamment sur :

- la faisabilité technique et fonctionnelle ;
- les estimations de charges, coûts et délais ;

- l'analyse des évolutions.

Toute demande fait l'objet d'une réponse formalisée dans un délai maximum de **cinq (5) jours ouvrés.**

Ces prestations s'exercent dans le seul périmètre applicatif de l'accord-cadre et sont rémunérées exclusivement par application des unités d'œuvre du bordereau des prix unitaires. Elles ne donnent lieu ni à la remise d'une offre, ni à une remise en concurrence, ni à l'établissement d'un devis exprimé en jours-homme ou selon toute autre unité étrangère au bordereau.

La réponse du titulaire ne constitue pas un devis : elle prend la forme d'une proposition de rattachement de la demande aux unités d'œuvre du bordereau, assortie de la justification du niveau de complexité retenu. Son élaboration n'est pas rémunérée, n'ouvre droit à aucune commande et ne peut donner lieu à facturation, y compris lorsque la DSI/DSAF renonce à commander la prestation. En cas de désaccord persistant sur le rattachement à une unité d'œuvre, la DSI/DSAF arrête l'unité d'œuvre applicable ; le point est inscrit à l'ordre du jour du comité de suivi le plus proche et, à défaut d'accord, du comité de pilotage.

Lorsque l'analyse conduit à engager une évolution, celle-ci est commandée, selon son ampleur, au titre de l'étude d'impact (article 7, poste 6) ou de la maintenance évolutive (article 6, poste 5).

### 2.10. Qualité et sécurité des développements

Le titulaire s'engage à respecter les bonnes pratiques de développement, notamment les normes de qualité logicielle, les exigences de sécurité et les standards des technologies utilisées.

Il met en œuvre des outils d'analyse permettant l'évaluation de la qualité et de la sécurité du code, la détection des vulnérabilités et le suivi des dépendances logicielles, et fournit les rapports associés à chaque livraison.

La DSI/DSAF se réserve le droit de faire auditer les livrables avant leur mise en production. Les anomalies identifiées lors de ces audits, résultant de choix techniques du titulaire à la date de la livraison, sont considérées comme des défauts imputables au titulaire et engageront sa seule responsabilité.

Cette disposition s'applique notamment, le cas échéant, aux situations suivantes :

- des configurations non conformes aux exigences techniques définies ;
- l'utilisation de composants logiciels obsolètes ou en fin de support ;
- l'utilisation de composants logiciels présentant des vulnérabilités « moyennes » ou « critiques/élevées » et exploitables ;
- la présence de vulnérabilités « majeures » ou « critiques » dans le code source, qu'elles soient directement exploitables ou non.

### 2.11. Accès aux environnements

Les environnements comprennent un environnement de recette, un environnement de préproduction et un environnement de production.

Les accès sont sécurisés et strictement encadrés. Aucune action d'administration à distance n'est autorisée.

Aucun accès direct en écriture à l'environnement de production n'est autorisé sans validation préalable.

## Article 3 - Prestation d'initialisation (Poste n°1)

### 3.1. Initialisation de la maintenance et prestations du périmètre initial (uo1)

#### 3.1.1. Description de la phase d'initialisation

La phase d'initialisation a pour objet de mettre en place les conditions opérationnelles d'exécution des prestations.
Le titulaire précise dans son offre la durée de cette phase, qui ne peut excéder **trois (3) mois** à compter de la notification de l'accord-cadre, la méthodologie retenue et le planning détaillé des activités.

Cette phase comprend notamment :

**a) Reprise du périmètre**

- transfert des activités de maintenance depuis les prestataires sortants ;
- organisation éventuelle d'une phase de réversibilité entrante ;
- prise en compte des applications à l'issue de la période de vérification de service régulier (VSR) le cas échéant.

**b) Mise en place des dispositifs contractuels**

- élaboration et validation des documents de référence :
  - Plan d'Assurance Qualité (PAQ) ;
  - Plan d'Assurance Sécurité (PAS) ;
  - plan de réversibilité ;
  - matrice des responsabilités.

Les modèles de ces documents sont fournis par la DSI/DSAF.

**c) Mise en place des outils**

- outil de gestion des incidents et demandes (soumis à validation de la DSI/DSAF) ;
- outil de gestion de configuration ;
- reprise des données issues des outils existants (Jira, Redmine, Mantis ou équivalent).

**d) Mise en place des environnements**

- installation des environnements de développement et d'intégration du titulaire ;
- prise en main des environnements de qualification ;
- vérification du bon fonctionnement des applications ;
- les environnements du titulaire doivent suivre le socle technique de la DSI/DSAF afin que les éléments des livraisons soient applicables au système d'information de la DSI/DSAF ;
- une réunion de restitution par le titulaire est organisée pour présenter l'environnement technique de travail. La DSAF/DSI se réserve le droit d'organiser une visite sur site du prestataire afin de valider ces éléments.

### e) Validation des processus

Afin de valider la bonne appropriation du périmètre, le titulaire réalise trois évolutions mineures incluses dans le prix des prestations.

### f) Gouvernance et organisation

- organisation de la réunion de lancement dans les deux semaines qui suivent la notification de l'accord-cadre ;
- mise en place des instances de pilotage ;
- définition du cadre méthodologique, des normes et des outils.

### g) Reporting et indicateurs

- mise en place des tableaux de bord de suivi d'activité (cf. articles 11.5 et 12.2) ;
- validation des indicateurs par la DSI/DSAF.

La phase d'initialisation débute à la date de notification de l'accord-cadre.

Sa réception est prononcée après validation des livrables et réalisation d'un bilan de fin de phase.

### h) Livrables attendus UO1

- plan d'assurance qualité (paq) ;
- plan d'assurance sécurité (pas) ;
- plan de réversibilité ;
- matrice des responsabilités ;
- mise en place des tableaux de bord de suivi d'activité (cf. article 12) ;
- bilan de fin de phase d'initialisation ;
- livrables des trois évolutions mineures réalisées au titre de la validation des processus ;
- documentation et livrables applicatifs conformes aux exigences des articles 11.6 et 11.7 ;
- compte rendu de la réunion de lancement ;
- compte rendu de la réunion de présentation de l'environnement technique ;
- désignation du référent accessibilité ;
- validation des indicateurs par la DSI/DSAF ;
- montage des environnements de développement ;
- référencement exhaustif des documents existants repris des sortants ;
- documentation contenant toutes les étapes de l'installation et configuration des environnements.

### 3.1.2. Périmètre initial

#### 3.1.2.1. Applications dites « standards » (lot 1)

Le périmètre initial comprend notamment les applications suivantes :

- AIVS
- AGLAE
- BASILIC
- BIVIA
- GESTION DES MANDATS
- PAGES BLANCHES

Les caractéristiques techniques détaillées sont précisées en annexe.

Ce périmètre est susceptible d'évoluer en cours d'accord-cadre.

#### 3.1.2.2. Applications basées sur les technologies ALFRESCO & NUXEO (lot 2)

Le périmètre initial comprend notamment les applications suivantes :

- ASGGARD : ConsMin, Espace Partagé, Gestion des contentieux, MEMORIM, RIM3
- SALSA 5
- SALSA BI

Les caractéristiques techniques détaillées sont précisées en annexe.

Ce périmètre est susceptible d'évoluer en cours d'accord-cadre.

#### 3.1.2.3. Sites internet & intranet (lot 3)

Le périmètre initial comprend notamment les sites suivants :

- https://www.academie-renseignement.gouv.fr/ (multisite)
- https://www.cada.fr/
- https://www.civs.gouv.fr/ (multisite)
- https://www.civen.fr/ (multisite)
- https://www.cncdh.fr/
- https://www.ccne-ethique.fr/ (lié à ccnen.fr avec Domain)
- https://www.ccnen.fr/( lié à ccne-ethique.fr avec Domain)
- https://www.cor-retraites.fr/
- https://www.csr-retraites.fr/ (multisite)
- https://www.diese.gouv.fr/
- https://www.dilcrah.gouv.fr/
- https://www.drogues.gouv.fr/
- https://www.educadroit.fr/
- https://www.harkis.gouv.fr/
- https://intranet.spm.rie.gouv.fr/
- https://www.strategie-plan.gouv.fr/

#### 3.1.2.4. Applications basées sur la technologie ODOO (lot 4)

Le périmètre initial comprend notamment les applications suivantes :

- Saveur

Les caractéristiques techniques détaillées sont précisées en annexe.

Ce périmètre est susceptible d'évoluer en cours d'accord-cadre.

## Article 4 - Prestations du socle : maintenance corrective et préventive (Poste n°2 - Volet 1)

### 4.1. Description des prestations

Les prestations du présent volet couvrent l'ensemble des applications du périmètre initial.

Elles comprennent :

- **UO2 : Maintenance corrective**, telle que définie à l'article 2.5 ;
- **UO3 : Maintenance préventive**, telle que définie à l'article 2.7.

### 4.2. Dimensionnement du poste – Maintenance corrective trimestrielle (UO2)

Le titulaire renseigne les éléments financiers dans le document d'annexe financière.

À ce titre, il doit notamment définir les charges en jours-homme selon les niveaux de complexité et les charges unitaires par type d'anomalie et niveau de criticité, renseigner les taux journaliers moyens (TJM) par profil, indiquer les prix annuels et les éléments du DQE.

Le titulaire s'engage sur un niveau de service, sur un niveau de productivité et sur une trajectoire de réduction des coûts.

Le prix couvre l'ensemble des prestations de maintenance corrective du périmètre initial sur la durée de l'accord-cadre.

**a) Livrables attendus UO2**

- un diagnostic des anomalies dans l'outil de suivi des tickets ;
- les correctifs des anomalies signalées, ou à défaut une solution de contournement temporaire ;
- le scénario, bilan et résultat des tests effectués, y compris les tests de non-régression et les tests de sécurité ;
- la mise à jour de la documentation existante, conformément aux exigences documentaires de l'article 11.6 ;
- la livraison des correctifs, conformément aux exigences applicatives de l'article 11.7 ;
- le rapport d'intervention ou d'incident sur demande de la DSAF dans les 48 heures suivant l'incident ;
- les impacts technico-fonctionnels sur le fonctionnement du service numérique ;
- Les éléments nécessaires à la mise à jour des cahiers de recette.

### 4.3. Dimensionnement du poste – Maintenance préventive (UO3)

Le titulaire renseigne également les éléments relatifs au maintien en conditions de sécurité dans l'annexe financière.

Il doit notamment définir les charges associées aux activités de veille, de sécurité et de maintien en condition, et compléter les éléments relatifs à l'UO3 dans les onglets prévus.

Le prix des prestations couvre l'ensemble des prestations de maintenance préventive sur le périmètre initial.

#### a) Livrables attendus UO3

- un rapport de sécurité mensuel ;
- un suivi des vulnérabilités.

### 4.4. Organisation des ressources

Le titulaire met en place une organisation adaptée au périmètre.

Il garantit :

- la disponibilité des compétences nécessaires ;
- la continuité de service ;
- la capitalisation des connaissances.

Des ressources dédiées sont affectées à la réalisation des prestations.

## Article 5 - Prestations hors socle (Poste 3 et poste 4 - Volet 2)

### 5.1. Maintenance corrective et préventive trimestrielle hors socle (UO4 à UO6)

#### 5.1.1. Définition du périmètre hors socle

Par périmètre hors socle, on entend l'ensemble des sites web et applications venant en complément du périmètre initial défini au volet 1.

La maintenance corrective couvre la prise en compte des demandes, les réponses aux demandes d'assistance, le maintien de la compétence et le pilotage de l'Activité. Elle est évaluée sur la base des abaques de charges (onglet « Abaques Charges »), à l'exclusion de l'historique des anomalies de l'année N-1.

Le maintien en conditions de sécurité est inclus dans les UO4 à UO6 et comprend :

- les revues de sécurité ;
- les contrôles de conformité ;
- le maintien en condition opérationnelle ;
- le maintien en conditions de sécurité ;
- le maintien de la compétence.

Elle est évaluée selon la complexité technique, sur la base des abaques.

**a) Livrables attendus UO4 à UO6**

- un diagnostic des anomalies dans l'outil de suivi des tickets ;
- les correctifs des anomalies signalées, ou à défaut une solution de contournement temporaire ;
- le scénario, bilan et résultat des tests effectués, y compris les tests de non-régression et les tests de sécurité ;
- la mise à jour de la documentation existante, conformément aux exigences documentaires de l'article 11.6 ;
- la livraison des correctifs, conformément aux exigences applicatives de l'article 11.7 ;
- les impacts technico-fonctionnels sur le fonctionnement du service numérique ;
- les éléments nécessaires à la mise à jour des cahiers de recette.
- les revues de sécurité ;
- les contrôles de conformité.

### 5.2. Résolution des anomalies (poste 4 : UO7 à UO15)

Les UO7 à UO15 permettent la prise en charge de la résolution des anomalies.

Chaque unité d'œuvre comprend :

- la gestion complète de **trois (3) tickets d'anomalie**, de la prise en compte à la résolution ;
- une valorisation basée sur :
    - la criticité de l'anomalie ;
    - la complexité technique du site web ou de l'application.

Un suivi trimestriel est réalisé sur la base d'un état des anomalies résolues.

**a) Livrables attendus UO7 à UO15**

- un diagnostic des anomalies dans l'outil de suivi des tickets ;
- les correctifs des anomalies signalées, ou à défaut une solution de contournement temporaire ;
- le scénario, bilan et résultat des tests effectués, y compris les tests de non-régression et les tests de sécurité ;
- la mise à jour de la documentation existante, conformément aux exigences documentaires de l'article 11.6 ;
- la livraison des correctifs, conformément aux exigences applicatives de l'article 11.7;
- les impacts technico-fonctionnels sur le fonctionnement du service numérique ;
- les éléments nécessaires à la mise à jour des cahiers de recette.

## Article 6 - Maintenance évolutive (Poste 5 : UO16 à UO18)

### 6.1. Définition

La maintenance évolutive vise à :

- faire évoluer les fonctionnalités ;
- améliorer les performances.

### 6.2. Nature des prestations

Elle comprend notamment :

- l'analyse d'impact et la définition de scénarios ;
- les évolutions techniques et fonctionnelles ;
- les développements ;
- l'intégration de services web ;
- les optimisations de performance.

### 6.3. Processus de mise en œuvre

- expression de besoin par les SPM ;
- analyse du titulaire (impact, charge, planning, coût) ;
- remise d'une proposition sous **cinq (5) jours ouvrés** ;
- émission d'un bon de commande ;
- réalisation de la prestation dès validation de la commande.

### 6.4. Réalisation des prestations

Les prestations comprennent :

- spécifications fonctionnelles et techniques ;
- développement ;
- tests ;
- livraison dans un environnement dédié afin de valider le DIN ;
- assistance à l'intégration, à distance ou sur site, au choix de la DSAF/DSI ;
- mise à jour de la documentation, à minima DCT, DEX, DIN, SFD, rapport d'audit RGAA.

### 6.5. Recette et validation

**a) Vérification d'aptitude (VA)**

- durée : 1 mois (sauf dérogation) ;
- validation via procès-verbal après correction des anomalies.

**b) Vérification de service régulier (VSR)**

- durée : 1 mois à partir de la décision positive de la vérification d'aptitude ;
- validation en conditions réelles d'exploitation.

### 6.6. Modalités de calcul

Le titulaire précise :

- l'unité d'œuvre utilisée ;

- la complexité associée.

Cette mention constitue un simple report : l'unité d'œuvre et le niveau de complexité sont ceux qui résultent de l'annexe financière et de la notation arrêtée par la DSI/DSAF dans les conditions de l'article 2.6. Aucune unité d'œuvre, charge ou prix ne figurant pas à l'annexe financière ne peut être retenu, ni aucun chiffrage exprimé en jours-homme. Toute mention non conforme est rectifiée par la DSI/DSAF lors de la constatation du service fait.

### 6.7. Livrables UO16 à UO18

- un devis détaillant la démarche technico-fonctionnelle ;
- les spécifications fonctionnelles et techniques ;
- le code source livré, conformément aux exigences applicatives de l'article 11.7 ;
- un rapport de sécurité (type Checkmarx ou équivalent) ;
- un cahier de tests (stratégie, non-régression, tests automatisés) ;
- mise à jour de la documentation, conformément aux exigences documentaires de l'article 11.6 ;
- procès-verbal de vérification d'aptitude (VA) ;
- validation de la vérification de service régulier (VSR).

## Article 7 - Étude d'impact ou d'analyse (poste 6 : UO19 à UO20)

### 7.1. Objet

Les études d'impact permettent :

- d'identifier les impacts sur le SI ;
- de proposer des scénarios ;
- de préparer les évolutions structurantes.

Les études d'impact relèvent de la validation de la DSAF/DSI.

L'appréciation de la faisabilité porte sur la faisabilité technique (compatibilité avec l'architecture existante, les versions supportées, les adhérences avec les applications partenaires et les contraintes d'hébergement), sur la faisabilité fonctionnelle (couverture du besoin exprimé, incidences sur les parcours utilisateurs, sur l'accessibilité numérique et sur les données) et sur la faisabilité opérationnelle (charge, délais, contraintes d'exploitation, de mise en production et de réversibilité). Chaque scénario est assorti d'une appréciation des risques et du degré de confiance de l'estimation associée. Lorsque la faisabilité n'est pas acquise, le titulaire l'indique expressément et énonce les conditions techniques ou fonctionnelles qui la rendraient possible.

L'étude d'impact ne constitue ni une consultation préalable, ni une remise en concurrence : elle porte exclusivement sur les applications et sites du périmètre de l'accord-cadre et son estimation est exprimée dans les seules unités d'œuvre du bordereau des prix unitaires, le titulaire justifiant le niveau de complexité retenu.

### 7.2. Typologie

- UO19 : étude simple, portant sur une demande dont les impacts sont circonscrits et identifiés et qui ne remet pas en cause l'économie générale du système, telle qu'un changement de version d'un composant sans adhérence avec les autres briques applicatives. La charge d'analyse est estimée à deux (2) jours ouvrés au maximum ;
- UO20 : étude complexe, portant sur une demande susceptible d'emporter des conséquences multiples devant être analysées systématiquement, notamment lorsqu'elle implique le changement d'un logiciel de base ou affecte plusieurs domaines fonctionnels ou plusieurs composants. La charge d'analyse est estimée à **cinq (5) jours ouvrés**.

### 7.3. Modalités

Le titulaire fournit la charge globale et sa répartition par profil.

Le titulaire remet le rapport d'étude dans un délai de **dix (10) jours ouvrés** à compter de la notification du bon de commande pour une étude simple (UO19) et de **vingt (20) jours ouvrés** pour une étude complexe (UO20), sauf délai différent expressément convenu avec la DSI/DSAF et mentionné au bon de commande. Le dépassement de ces délais donne lieu à l'application des pénalités prévues au CCAP.

La DSI/DSAF dispose de **dix (10) jours ouvrés** à compter de la remise du rapport pour le valider, demander un complément ou le rejeter par décision motivée. Lorsqu'un complément est demandé, le titulaire le remet dans un délai de **cinq (5) jours ouvrés** ; ce délai suspend le délai de validation. La conclusion de l'étude, y compris lorsqu'elle établit que l'évolution envisagée n'est pas réalisable ou n'est pas opportune, est sans incidence sur la rémunération de l'unité d'œuvre commandée, dès lors que le rapport comporte l'ensemble des éléments attendus.

L'estimation en unités d'œuvre figurant au rapport engage le titulaire pendant une durée de **six (6) mois** à compter de la validation de celui-ci. Les travaux qui en découlent sont commandés, dans ce délai, sur la base de cette estimation, sans que le titulaire puisse en demander la revalorisation, sauf modification du besoin exprimée par la DSI/DSAF ou évolution des conditions techniques dûment constatée et acceptée par elle.

### 7.4. Livrables attendus UO19 à UO20

- devis de la prestation ;
- rapport de l'étude d'impact et de faisabilité ;
- estimations des UO de conception/développement découlant de l'étude ;
- planning prévisionnel des opérations découlant de l'étude ;
- analyse d'impact sur les documents existants et scénarios de tests.

## Article 8 - Entrée d'un nouveau site web ou d'une application dans le périmètre (poste 7 : UO21 à UO23)

### 8.1. Objet

Permet l'intégration d'un nouveau site web ou d'une application dans le périmètre pour une durée de **12 mois** renouvelable de façon tacite.

### 8.2. Phase préalable

La DSI peut demander au titulaire, préalablement à l'émission d'un bon de commande, une analyse de la demande d'intégration d'un nouveau site ou d'une nouvelle application.

Le titulaire fournit une estimation de la charge, un planning et une proposition financière permettant à la DSI d'émettre le bon de commande afférent. La proposition financière est établie par application exclusive de l'annexe financière : il se borne à identifier les UO nécessaires à la réalisation de la demande.

### 8.3. Prise en charge

La prise en charge comprend la prise de connaissance, l'installation sur les environnements, le diagnostic, la mise en place des outils de suivi et la montée en compétence.

Le titulaire doit démontrer sa capacité via la réalisation de deux évolutions mineures.

### 8.4. Livrables attendus UO21 à UO23

- analyse du besoin ;
- estimation de charge, planning et proposition financière (phase préalable) ;
- livrables des deux évolutions mineures réalisées pour démontrer la capacité de prise en charge ;
- documentation et livrables applicatifs conformes aux exigences des articles 11.6 et 11.7 ;
- comptes rendus des ateliers et réunions de prise de connaissance ;
- montage des environnements et documentation des étapes d'installation et de configuration.

## Article 9 - Prestations ponctuelles de TMA hors périmètre (Poste 8 : UO24 à UO26)

### 9.1. Objet

Ces prestations sont des interventions ponctuelles sur des applications ou sites hors périmètre.

### 9.2. Modalités

- étude préalable (UO19) obligatoire ;
- définition de l'UO adaptée ;
- formalisation via un protocole d'intervention.

### 9.3. Livrables attendus UO24 à UO26

- l'étude préalable (UO19) est obligatoire ;
- devis de la prestation ;
- comptes rendus de réunions de travail ;
- planning de mise en œuvre ;
- rapport d'expertise/d'intervention ;

- mise à jour des documentations existantes, conformément aux exigences documentaires de l'article 11.6 ;
- le cas échéant, la livraison des correctifs ou évolutions réalisés, conformément aux exigences applicatives de l'article 11.7.

## Article 10 - Réversibilité (Poste 9 : UO27 à UO30)

### 10.1. Objet

La réversibilité renvoie à l'organisation du transfert vers un autre prestataire ou vers la DSI ou une fin de vie.

### 10.2. Types

- réversibilité partielle (site/application) ;
- réversibilité globale (fin d'accord-cadre) ;
- fin de vie : transmission des livrables pour archivage.

### 10.3. Contenu

Le titulaire transfère les connaissances, fournit l'ensemble des livrables et des codes et accompagne le repreneur.

### 10.4. Délais

- simple/moyen : 1 mois avec 5 ateliers de 2 heures ;
- complexe : 2 mois avec 10 ateliers de 2 heures ;
- périmètre initial : 2 mois avec 10 ateliers de 2 heures.

### 10.5. Livrables attendus UO27 à UO30

- l'ensemble des codes sources applicatifs, déposés et transmis selon les modalités de l'article 11.7 ;
- l'ensemble de la documentation des produits et services numériques à jour ;
- plan de réversibilité détaillé (méthodologie + calendrier) ;
- liste des tickets restant à traiter ;
- récapitulatif exhaustif de la documentation/sources/outils livrés ;
- scripts d'exploitation et de tests automatisés ;
- rapports de sécurité (type Checkmarx ou équivalent).

## Article 11 - Exigences et engagements

### 11.1. Exigences de sécurité

#### 11.1.1. Conformité à l'état de l'art

Le titulaire conçoit, met en œuvre et exploite les systèmes conformément à l'état de l'art en matière de sécurité des systèmes d'information, notamment selon les recommandations de l'ANSSI.

**Exigences applicables aux interfaces web et applications :**

- absence de dépendance à des technologies obsolètes (notamment Adobe Flash, Microsoft Silverlight ou un environnement d'exécution Java ne bénéficiant plus d'un support de sécurité de son éditeur) ;
- utilisation obligatoire du protocole TLS (HTTPS), version 1.3 recommandée ;
- recommandation d'utilisation de HSTS ;
- contrôle de sécurité sur les types de données côté serveur ;
- sécurisation des cookies (HttpOnly, Secure, SameSite) ;
- mise en œuvre des en-têtes de sécurité (CSP, SRI, X-Frame-Options, etc.) ;
- respect des obligations légales d'information ;
- éviter l'usage des websockets ;
- authentification par SSO.

**Exigences applicables aux services de messagerie :**

- chiffrement de l'ensemble des flux de messagerie, notamment au moyen des protocoles STARTTLS, SMTPS et IMAPS.
- mise en œuvre des mécanismes :
    - SPF
    - DKIM
    - DMARC

#### 11.1.2. Gestion des biens et des données

Le titulaire garantit :

- la séparation stricte des données entre clients ;
- l'accès limité au strict besoin d'en connaître ;
- la protection des supports physiques (stockage sécurisé, destruction contrôlée) ;
- la confidentialité des échanges d'informations ;
- l'innocuité des supports échangés ;
- la traçabilité des transferts (registre des échanges) ;
- le marquage des ressources sensibles ;
- la destruction sécurisée des supports en fin de vie ;
- la mise à disposition complète des données à l'acheteur ;
- la transmission d'informations de l'administration (code source, éléments de documentation, contexte, etc…) à une source tierce (exemples : intelligence artificielle générative, service d'analyse de code en ligne) doit être soumise à une autorisation formelle du pouvoir adjudicateur.

En outre, tout incident de sécurité doit être communiqué sans délai à la DSAF.

#### 11.1.3. Sécurité du poste de travail

Le titulaire doit protéger l'accès physique à ses postes de travail comme à ses supports de stockage. Il met en œuvre des dispositifs destinés à interdire leur accès à des acteurs externes, à retarder le vol des matériels ou à assurer le niveau de confidentialité attendu. Les mesures associées sont le verrouillage des bureaux, la présence d'armoires fermant à clef, l'installation de filtres de confidentialité sur les écrans ou encore l'activation du verrouillage de session après une période d'inactivité.

Le titulaire s'assure que ses postes de travail sont dotés d'une solution de protection contre les codes malveillants (type antivirus) disposant en permanence des dernières mises à jour de son éditeur.

Il met en place un pare-feu local sur les postes de travail interdisant tous les flux entrants.

Il met en œuvre des mesures de chiffrement surfacique de ses postes nomades et autres supports de stockage « perdables ».

Il précise sa politique de durcissement et de spécialisation de ses postes de travail, laquelle intègre la nécessité de limiter ou d'interdire les postes partagés ou multiniveaux, l'application du principe du moindre privilège et la nécessité de limiter ou d'interdire le recours à des comptes génériques.

#### 11.1.4. Conformité, audit et contrôle

Le titulaire :

- réalise des autocontrôles réguliers ;
- met en œuvre un plan de remédiation sous **quinze (15) jours ouvrés** en cas d'écart ;
- corrige les non-conformités dans les délais convenus.

### 11.2. Exigences liées aux prestations d'étude

Le titulaire :

- applique les standards et méthodes de l'acheteur ;
- réalise les analyses de risques SI ;
- respecte la ségrégation des environnements (dev / recette / préprod).

Les tests sont conduits à partir de données anonymisées, sans impact sur le système d'information, et les environnements sont remis en état à leur issue.

### 11.3. Exigences liées aux développements

Le titulaire respecte :

- le cadre de développement de l'acheteur ;
- Le cadre initial de l'application ;

- les outils et frameworks préconisés.

**Obligations :**

- propriété du code transférée à l'acheteur ;
- protection des codes sources ;
- documentation systématique de tous les élément du code au déploiement et l'exploitation ;
- traçabilité des développements ;
- sauvegarde et versionning des codes :
    - Gestion sémantique de version : « A.B.C » avec :
        - A = version majeure du produit ;
        - B = version MCO du produit (correction fonctionnelle) ;
        - C = correction bug ou MCS du produit.
- Notes relatives aux changements réalisés dans la version livrée
- dépôt conforme aux exigences de l'acheteur ;
- code variabilisé, utilisation de fichiers d'environnements ;
- mise en place et configuration des logs afin de répondre aux exigences de la DSI/DSAF.

**Tests et qualité :**

- tests sans perturbation du SI ;
- absence de régression ;
- utilisation de données anonymisées ;
- production de rapports qualité/sécurité mensuel ainsi qu'à chaque livraison.

**Contrôles :**

La DSI réalise des audits de code et des tests d'intrusion.

#### 11.3.1. Inventaire des composants

Le titulaire fournit :

- un rapport de sécurité (type Checkmarx ou équivalent) mensuel ainsi qu'à chaque livraison :
    - incluant l'exhaustivité des versions et composants (librairies, plugins…) : format SBOM recommandé ;
    - avec recommandations de mise à jour ;
    - une analyse motivée du rapport de sécurité (justifications des faux positifs éventuels, mesures d'atténuations, etc.).

## 11.4. Exigences relatives au personnel

### 11.4.1. Qualifications et expérience

- équipes en capacité d'intervenir dans les locaux de l'administration à la demande écrite de la DSI/DSAF, à leurs frais, dans un délai de **quarante-huit (48) heures**, y compris en cas de gestion de crise ou d'incident de sécurité ; compte tenu de la sensibilité des systèmes concernés et des exigences de l'article 1.1.4, les prestations donnant accès aux environnements, aux codes sources ou aux données sont exécutées depuis le territoire d'un État membre de l'Union européenne, le titulaire indiquant ce lieu dans son offre, toute modification étant soumise à l'accord préalable écrit de la DSI/DSAF ;
- intervenants expérimentés par périmètre ;
- compétences techniques adaptées (web et applicatif, accessibilité numérique) ;
- tous les contributeurs ou les personnes accédant au code source doivent être identifiés nominativement et être couvert par un contrat pour cette usage auprès du titulaire ;
- en outre, toute modification du code source doit être imputable à une personne identifiée.

**Remplacement des ressources :**

- profils équivalents exigés
- validation préalable par l'acheteur

Le titulaire présente l'organisation mise en place pour pallier le départ d'une ressource.

**Confidentialité :**

- signature obligatoire d'un engagement de confidentialité

Les modalités de remplacement sont indiquées dans l'article 8.2.2 du CCAP.

### 11.4.2. Gestion des ressources

Le titulaire décrit l'organisation des équipes, la mutualisation des compétences, la gestion des charges, le recours à la sous-traitance et la gestion des entrées et des sorties.

Il s'engage sur la continuité de service et sur le transfert de compétences en cas de remplacement.

## 11.5. Convention de niveau de service (CNS)

### 11.5.1. Définition des sévérités

| Sévérité | Définition |
|---|---|
| **1 – Bloquante** | Impact critique sur une fonction essentielle |

| Sévérité | Définition |
|---|---|
| **2 – Majeure** | Impact significatif avec contournement possible |
| **3 – Mineure** | Impact faible sans blocage |

### 11.5.2. Délais de traitement

**Définitions :**

- **d1** : prise en compte ;
- **d2** : solution de contournement ;
- **d3** : correction.

**Règles :**

- déclenchement via ticket ou email ;
- délais en heures/jours ouvrés (8h–19h) ;
- possibilité de délais définis au bon de commande .

### 11.5.3. Niveaux de service attendus

| Gravité | d1 | d2 | d3 |
|---|---|---|---|
| Bloquante | 4h | 1 jour | 5 jours |
| Majeure | 1 jour | 3 jours | 10 jours |
| Mineure | 5 jours | - | jusqu'à 20 jours |

### 11.5.4. Mesure des délais

Anomalie : temps X

- calcul basé sur le temps d'affectation au titulaire
- exclusions :
  - attente SPM ;
  - phases de recette ;
  - blocages imputables à l'acheteur.

### 11.5.5. Interventions hors horaires

Le titulaire propose :

- majorations pour interventions :
  - hors heures ouvrées ;

- week-end et jours fériés.

Les heures non ouvrées s'entendent des heures antérieures à 8 heures et postérieures à 19 heures ; les majorations de week-end et de jours fériés s'appliquent de 8 heures à 19 heures. Les taux de majoration sont exprimés en pourcentage du prix de l'unité d'œuvre concernée et renseignés au bordereau des prix unitaires pour les unités d'œuvre UO7 à UO18 et UO24 à UO26. Aucune majoration ne s'applique aux autres unités d'œuvre. Toute intervention hors horaires est préalablement autorisée par écrit par la DSI/DSAF.

## 11.6. Livraison et validation des documents

### 11.6.1. Modalités de livraison

- documentation complète (DCT, DIN, DEX, rapport d'audit RGAA à jour systématiquement fournies) ;
- ensemble des rapports avec les résultats des tests de qualité et de sécurité mentionnés aux articles 11.1 et 11.3 ;

- Ces éléments doivent être chiffrés via un outil qualifié ANSSI suivant le mode de transfert au choix de la DSI :
  - email via conteneur ZED (ou équivalent) ;
  - Mise à disposition sur un accès Web protégé.

### 11.6.2. Validation

- validation conjointe titulaire / SPM ;
- possibilité de consultation des experts DSI.

## 11.7. Livraison des composants logiciels

### 11.7.1. Mise en production

À chaque livraison :

- livraison des sources (code, dockerfile et scripts de déploiement si applicable) sur GIT SPM ;
- livraison des binaires. La transmission doit être chiffrée via un outil qualifié ANSSI suivant le mode de transfert au choix de la DSI :
  - email via conteneur ZED (ou équivalent) ;
  - Mise à disposition sur un accès Web protégé.
- scripts nécessaires au déploiement fournis et variabilisés ;
- assistance au déploiement ;
- Les livraisons doivent permettre le déploiement dans l'environnement de la DSAF/DSI via une chaine de déploiement automatisée par application.

### 11.7.2. Validation de sécurité

Une analyse technique de chaque livraison est réalisée par le pouvoir adjudicateur.

Cette analyse peut donner lieu à un rejet motivé de la livraison (présence de vulnérabilités critiques ou nombreuses, composants dont le support éditeur a pris fin).

### 11.8. Gestion des demandes et incidents

#### 11.8.1. Outil de gestion des tickets

Le titulaire met en place un outil :

- accessible en ligne ;
- par périmètre ;
- avec export standard ;
- non propriétaire.

#### 11.8.2. Qualification des anomalies

**Anomalies applicatives :**

- classification selon sévérité ;
- qualification par la DSI/DSAF en lien avec le métier ;
- arbitrage DSI en cas de désaccord.

**Anomalies documentaires :**

| Niveau | Description |
|---|---|
| Bloquante | empêche l'exploitation |
| Majeure | incohérences importantes |
| Mineure | défauts mineurs |

#### 11.8.3. Cycle de vie des incidents

- création du ticket ;
- affectation ;
- traitement ;
- validation par SPM ;
- clôture ;
- possibilité de réouverture.

## Article 12 - Organisation et responsabilités

### 12.1. Les rôles et responsabilités

#### 12.1.1. L'entité des SPM responsable du site web ou de l'application

L'entité des SPM souhaitant bénéficier de l'accord-cadre est représentée par un responsable d'application (chef de projet), disposant de compétences fonctionnelles.

À ce titre, il assure notamment :

- la validation des livrables documentaires de la TMA ;
- les tests en qualification ;
- les tests en pré-production et la validation des développements ;
- la validation des demandes de déploiement ;
- une assistance de niveau 2 aux utilisateurs ;
- l'animation du réseau des correspondants utilisateurs ;
- la formation interne ;
- la gestion et la priorisation des évolutions ;
- la définition des niveaux et objectifs de qualité de service ;
- la représentation de la maîtrise d'ouvrage dans les instances de gouvernance.

La DSI précise, lors de chaque entrée dans le périmètre, si ce rôle est porté par l'entité SPM ou par elle-même.

#### 12.1.2. La DSI/DSAF - Responsable contractuel

La DSI/DSAF :

- assure le pilotage global de l'accord-cadre ;
- garantit le bon fonctionnement de la TMA ;
- arbitre les priorités, délais et coûts ;
- coordonne les actions avec le titulaire ;
- suit les engagements contractuels et budgétaires ;
- participe aux instances de gouvernance.

#### 12.1.3. Répartition des rôles

**Direction DSI/DSAF :**

- suit le pilotage global du contrat ;
- assure le premier niveau d'escalade en cas de litige.

**DSAF (Direction / BAM) :**

- gère les aspects administratifs et juridiques de l'accord-cadre ;
- assure la passation et le suivi des marchés.

**Chef de bureau / Product Manager :**

- pilote le contrat ;
- suit les indicateurs de qualité ;
- prépare les comités ;
- assure le reporting aux SPM.

**DSI/DSAF :**

- coordonnent les activités de maintenance ;
- qualifient les demandes ;
- pilotent les évolutions ;
- organisent les recettes ;
- suivent les déploiements ;
- veillent au respect des normes ;
- coordonnent les acteurs ;
- participent aux comités ;
- proposent les décisions d'admission.

## 12.2. Gouvernance et pilotage

Deux instances structurent la gouvernance :

- comité de suivi (COSUI) ;
- comité de pilotage (COPIL).

Les comités sont organisés distinctement pour les périmètres :

- sites web / intranet (lot 3) ;
- applications dites standards (lot 1) ;
- applications ALFRESCO / NUXEO (lot 2) ;
- Odoo (lot 4).

Le titulaire :

- propose les ordres du jour ;
- rédige les comptes rendus (validation DSI/DSAF).

Les modalités sont précisées dans le PAQ.

L'ordre du jour de chaque instance est arrêté conjointement par la DSI/DSAF et le titulaire ; le titulaire en établit la proposition et la transmet dans les délais propres à chaque instance fixés ci-après. Le titulaire rédige le compte rendu de chaque séance selon le modèle transmis par la DSI/DSAF ; la DSI/DSAF dispose de **deux (2) jours ouvrés** à compter de sa réception pour formuler ses observations, à défaut de quoi le compte rendu est réputé validé.

### 12.2.1. Le Comité de suivi (COSUI)

Le comité de suivi a pour objectifs le suivi opérationnel de la TMA, le pilotage des évolutions, la gestion des incidents, la validation des devis, la planification des livraisons et le suivi des risques.

Le comité de suivi se réunit chaque semaine, ainsi qu'à la demande de la DSI/DSAF ou du titulaire dès que le besoin en est exprimé par l'une ou l'autre partie. Il se tient à distance, sauf demande contraire de la DSI/DSAF.

Le comité de suivi se tient à distance, sauf demande contraire de la DSI/DSAF. Le titulaire transmet la proposition d'ordre du jour et le support de réunion au moins un (1) jour ouvré avant la séance ; le compte rendu est établi dans les **trois (3) jours ouvrés** suivant la séance.

En cas de situation urgente, notamment d'incident de production, d'incident de sécurité ou de crise, la DSI/DSAF peut convoquer une réunion exceptionnelle avec un délai de prévenance de **quarante-huit (48) heures**. Le titulaire assure la présence des intervenants requis, y compris dans les locaux de l'administration lorsque la DSI/DSAF le demande, sans frais supplémentaires pour l'acheteur.

**Participants :**

- DSI/DSAF (product owner, product manager senior, responsables) ;
- SPM (si nécessaire) ;
- Titulaire (chef de projet + équipe).

**Livrables**

- support de réunion selon le modèle transmis par la DSAF/DSI ;
- compte rendu **établi dans les trois (3) jours ouvrés suivant la séance.**

### 12.2.2. Le Comité de Pilotage (COPIL)

Le comité de pilotage assure le pilotage stratégique de l'exécution, l'arbitrage des priorités et des enveloppes, le suivi des engagements contractuels, l'analyse de la qualité des prestations et l'orientation de la TMA. Il tranche les points que le comité de suivi n'a pas résolus.

Le comité de pilotage se réunit chaque trimestre, cette périodicité pouvant être adaptée en fonction des contraintes du projet. Il est convoqué par la DSI, qui en arrête la date au moins **dix (10) jours ouvrés** avant la séance. Il se tient dans les locaux de l'administration ou à distance, au choix de la DSI.

Le titulaire transmet la proposition d'ordre du jour et le support de présentation à la DSI/DSAF au moins **trois (3) jours ouvrés** avant la séance. La DSI/DSAF formule ses observations dans les **deux (2) jours ouvrés** suivant la réception ; le titulaire diffuse la version définitive du support aux participants au plus tard **un (1) jour ouvré** avant la séance.

Le support comporte au minimum :

- le bilan de la période écoulée, par unité d'œuvre commandée, exécutée et facturée ;
- l'état d'avancement des évolutions en cours et le respect des jalons ;
- le suivi des indicateurs de la convention de niveau de service et l'analyse des écarts constatés ;
- l'état du stock d'anomalies par niveau de sévérité et son évolution ;
- le suivi de la consommation financière au regard du montant maximum de l'accord-cadre ;
- le suivi des engagements pris lors des séances précédentes ;
- l'état d'avancement de la clause sociale d'insertion et des engagements environnementaux ;
- les risques identifiés, les mesures de traitement proposées et les points appelant un arbitrage de la DSI.

Le titulaire adresse à la DSI, un relevé de décisions dans les **deux (2) jours ouvrés** suivant la séance, puis le compte rendu complet, établi selon le modèle transmis par la DSI, dans les **trois (3) jours ouvrés**. La DSI dispose de **deux (2) jours ouvrés** à compter de la réception pour formuler ses observations ; à défaut, le compte rendu est réputé validé.

Un comité de pilotage exceptionnel est convoqué à l'initiative de la DSI/DSAF avec un délai de prévenance de **cinq (5) jours ouvrés**, notamment en cas de non-respect des engagements de la convention de niveau de service sur deux périodes consécutives, d'incident de sécurité majeur, de dérive constatée de la consommation financière ou de désaccord persistant sur le rattachement d'une demande à une unité d'œuvre.

Le comité de pilotage suivant la date anniversaire de la notification de l'accord-cadre est consacré au bilan annuel de l'exécution. Le titulaire y rend compte de l'atteinte du niveau de productivité et de la trajectoire de réduction des coûts sur lesquels il s'est engagé au titre de l'article 4.2 du présent document, du bilan de la clause sociale d'insertion et de la mise à jour du plan d'assurance qualité. Il y présente, le cas échéant, sa demande de révision des prix, sans que cette présentation le dispense des formalités prévues par l'article du CCAP relatif à la variation des prix.

**Participants.** Y participent les directions des SPM concernées, la DSI/DSAF et, pour le titulaire, sa direction ainsi que le chef de projet. Le titulaire y est représenté par une personne habilitée à l'engager. Toute absence est consignée au compte rendu.

**Récapitulatif des délais applicables au comité de pilotage :**

| Étape | À la charge de | Délai |
|---|---|---|
| Fixation de la date de la séance | DSI | 10 jours ouvrés avant la séance |
| Proposition d'ordre du jour et support de présentation | Titulaire | 3 jours ouvrés avant la séance |
| Observations sur l'ordre du jour et le support | DSI | 2 jours ouvrés à compter de la réception |
| Diffusion du support définitif aux participants | Titulaire | 1 jour ouvré avant la séance |
| Relevé de décisions | Titulaire | 2 jours ouvrés après la séance |
| Compte rendu de séance | Titulaire | 3 jours ouvrés après la séance |
| Observations sur le compte rendu | DSI | 2 jours ouvrés à compter de la réception ; à défaut, compte rendu réputé validé |
| Convocation d'une séance exceptionnelle | DSI | 5 jours ouvrés de prévenance |

**Livrables :**

- Support de réunion selon le modèle transmis par la DSAF/DSI ;
- Compte rendu établi dans les **trois (3) jours ouvrés** suivant la séance.

## Article 13 - Plan qualité du projet et des prestations

### 13.1. Plan d'Assurance Qualité (PAQ)

Le titulaire fournit un PAQ initial décrivant l'organisation et les processus mis en œuvre.
Ce document est validé par la DSI, s'applique à l'ensemble du périmètre et peut être complété par des annexes spécifiques à chaque application ou site.

**Contenu du PAQ**

Le PAQ précise notamment :

- les livrables associés à chaque prestation ;
- les processus de tests et de validation ;
- les indicateurs de qualité ;
- le tableau de bord de suivi ;
- le journal des événements ;
- les rôles et responsabilités ;
- les modalités de gestion documentaire et logicielle ;
- les processus de mise à jour ;
- les protocoles spécifiques (maintenance ponctuelle, mode projet) ;
- les éventuelles dérogations spécifiques.

### 13.2. Suivi de la qualité des prestations

La DSI/DSAF peut réaliser ou faire réaliser des audits, demande les résultats des tests de qualité et vérifie le respect du PAQ.

Le titulaire supporte l'impact des audits, fournit un planning détaillé, propose des indicateurs de performance et garantit le suivi des engagements contractuels.

## Article 14 - ANNEXES

### 14.1. Politique de sécurité des systèmes d'information de l'État (PSSIE) (annexe 1)

La politique de sécurité des systèmes d'information de l'État est disponible à l'adresse suivante : Politique de sécurité des systèmes d'information de l'Etat - Légifrance

### 14.2. Le cadre de cohérence technique (annexe 2)

Le cadre de cohérence technique n'est pas joint au dossier de consultation en raison de son caractère sensible ; il est communiqué aux candidats qui en font la demande, après signature de l'engagement de confidentialité annexé au règlement de la consultation.

### 14.3. Volet initial : liste du parc applicatif initial de l'accord-cadre TMA des sites internet et applications (annexe 3)

Ces documents listent l'ensemble du parc applicatif à prendre en compte pour le volet initial :

- du lot 1 : 26_BAM_836_CCTP_Annexe 3_Lot1_Appli_volet_initial.docx
- du lot 2 26_BAM_836_CCTP_Annexe 3_Lot2_Alfresco-NUXEO_volet initial.docx
- du lot 3 : 26_BAM_836_CCTP_Annexe 3_Lot3_Web_volet_initial.docx
- du lot 4 : 26_BAM_836_CCTP_Annexe 3_Lot4_ODOO_volet_initial.docx

### 14.4. La matrice de complexité (annexe 4)

Ce document est une matrice simplifiée. Il figure dans le dossier de consultation.