



MINISTÈRE
CHARGÉ DE LA MER
ET DE LA PÊCHE

*Liberté
Égalité
Fraternité*

DGAMPA
SDTNUM

Marché de tierce maintenance applicative

Cahier des Clauses Techniques
Particulières

Version 1.0

Historique des versions du document

Version	Date	Commentaire
0.1	30/05/2025	Version initiale
0.2	24/06/2025	Relecture et correction
0.3	30/08/2025	Relecture et correction
0.4	23/09/2025	Consolidation
1.0	08/10/2025	Version finale

Affaire suivie par

Patrick BARUSSEAU – SDTNUM/DGAMPA
Tél. : +33 2 99 19 60 43 /
Courriel : patrick.barusseau@mer.gouv.fr

Rédacteur

Patrick BARUSSEAU – SDTNUM/BPN

Relecteur

Arnaud Morel – SDTNUM/BPN

Alexandra MENIS – SDTNUM /CPBG

SOMMAIRE

01. PRESENTATION GENERALE DU MARCHE	5
1.1 Présentation du document	5
1.2 Objet du marché	5
1.3 Durée du marché	5
1.4 Périmètre du marché	5
1.5 Compatibilité des prestations de maîtrise d'œuvre du présent marché et d'éventuelles prestations d'AMOA	6
1.6 Lieu d'exécution des prestations	6
02. CONTEXTE ET ORGANISATION	8
2.1 Présentation de la DGAMPA	8
2.2 Missions et organisation de la Sous-Direction de la transformation Numérique (SDTNUM)	8
03. REFERENTIEL QUALITE ET SECURITE	10
3.1 PAQ et PAS	10
3.2 Réglementation	11
3.3 Cadre normatif et exigences de sécurité	11
3.4 Communication des incidents de sécurité	13
3.5 Publication de vulnérabilité – Attaques – Actions de prévention	13
3.6 Audit	14
3.7 Cadre technique	14
3.8 Analyse statique de la qualité et de la sécurité du code	15
3.9 Résorption de la dette technique	15
3.10 Conditions spécifiques liées à l'usage de l'Intelligence Artificielle	15

3.11 Licences logicielles et dépendances	16
04. MODALITES D'EXECUTION DU MARCHE	16
4.1 Principes généraux de gouvernance du marché	16
4.2 Suivi contractuel et pilotage général	17
4.3 Instances de suivi opérationnel des prestations	18
4.4 Processus relatif à la réception des livrables	19
4.5 Admission des livrables conditionnée par une réception, suivie d'une vérification d'aptitude (VA) et une vérification du service régulier (VSR)	20
4.6 Admission conditionnée par une réception suivie d'une validation documentaire	21
4.7 Admission conditionnée par une constatation mensualisée	22
4.8 Portage d'expertise indépendante	22
4.9 Réversibilité et transférabilité	23
4.10 Gestion du turn-over	23
4.11 Formation et qualification des ressources proposées par le Titulaire	25
4.12 Les horaires de travail	25
05. DESCRIPTION DES PRESTATIONS ATTENDUES	26
5.1 Les prestations et unités d'œuvre du marché	26
5.2 Outillage de gestion	27
5.3 Notion d'anomalie	27
06. PROFIL DES INTERVENANTS	29

01. Présentation générale du marché

1.1 Présentation du document

Le présent marché de tierce maintenance applicative (TMA) est un marché à bons de commande.

Le bénéficiaire de ce marché est la Sous-Direction de la Transformation Numérique (SDTNUM) de la Direction générale des affaires maritimes de la pêche et l'aquaculture (DGAMPA) dénommée Personne Publique dans la suite du document.

Ce document constitue le CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP) du marché. Il décrit les caractéristiques et modalités techniques des prestations prévues au titre de la TMA.

1.2 Objet du marché

La Personne Publique, en tant que maître d'œuvre, souhaite recourir à une assistance externe pour la maintenance préventive, corrective et évolutive des produits numériques dont elle a la charge pour le compte de ses services. Les technologies utilisées pour réaliser ces produits sont précisées en annexe 3.

Les produits sont développés et maintenus selon des méthodes cycle en V, en méthode agile ou mode produit (mode agile avec pilotage par l'impact). Le modèle opérationnel agile est décrit en annexe 4.

1.3 Durée du marché

Le marché, qui doit être notifié avant tout commencement d'exécution, est conclu pour une durée de deux ans, reconductible tacitement deux fois un an, à compter du jour de sa notification.

En cas de non reconduction, l'Administration est tenue de le notifier au titulaire au plus tard soixante jours ouvrés avant l'échéance de fin.

1.4 Périmètre du marché

Le présent marché couvre des prestations de maintenance applicative ainsi que des prestations d'opérations techniques, d'audits, d'expertises et d'accompagnement. Le périmètre initial des produits numériques concernés est indiqué pour information en annexe 3.

Les applications du périmètre feront l'objet de commande spécifique comprenant l'initialisation la prise en charge par le titulaire avant tout commencement des travaux : cf. unité d'œuvre UO_PCHA.

Le périmètre est susceptible d'évoluer en cours du marché :

- Certaines applications peuvent sortir du périmètre à la demande de la personne publique, notamment en cas de dé-commissionnement. La sortie d'une application du périmètre du marché n'ouvre droit à aucune indemnité.
- Certaines applications peuvent être ajoutées au périmètre à la demande de la personne publique. Ces cas feront alors l'objet de commande spécifique d'initialisation et de prise en charge (unité d'œuvre UO_PCHA).

1.5 Compatibilité des prestations de maîtrise d'œuvre du présent marché et d'éventuelles prestations d'AMOA

Le représentant du pouvoir adjudicateur (RPA) attire l'attention des candidats sur le fait qu'il n'accepte pas, en règle générale, qu'un prestataire agissant pour son compte soit à la fois AMOE et AMOA pour un même produit numérique

Par conséquent, s'il s'avère que le candidat retenu au présent marché assure par ailleurs pour le compte du RPA des prestations d'AMOA via un autre marché, celles-ci ne seront pas maintenues au terme d'une période n'excédant pas six mois à compter de la notification du présent marché.

Le titulaire ne pourra réaliser de prestation d'AMOA pour le compte de la SDTNUM dans le cadre de produit du périmètre du présent marché.

1.6 Lieu d'exécution des prestations

Les prestations seront localisées en France voire dans l'Union Européenne.

Elles seront réalisées :

- Soit dans les locaux du Titulaire et dans ce cas elles tiendront compte des contraintes suivantes :
 - Impératifs de sécurité (sécurité du réseau, confidentialité due par les intervenants, sécurité des accès physiques aux locaux) ;
 - Capacité que doit avoir à tout moment la Personne Publique à effectuer des audits sur place, afin de s'assurer du respect des normes, règles et exigences qui s'imposent au titulaire ;
 - Garantie de continuité de service.

En outre, les locaux du Titulaire dans lesquels seront réalisées les prestations du marché devront se situer à une distance des locaux de la Personne Publique, y compris ceux situés hors Île de France, pour privilégier l'aller-retour dans la journée.

- Soit dans les locaux de la Personne Publique avec mention expresse dans le bon de commande. Dans ce cas, les règles de fonctionnement définies par la Personne Publique s'appliqueront aux collaborateurs du Titulaire.

Cette notion de lieu de réalisation doit être entendue sur les plans contractuels et organisationnels. En pratique, le collaborateur du Titulaire pourra également assurer sa mission en présentiel, ou télétravail, sous réserve de l'accord de la personne Publique.

Dans le cas où l'intervenant du titulaire, validé par la Personne publique, doit se rendre sur un site de la Personne publique, différent du lieu de travail habituel convenu de l'intervenant, il sera possible de dédommager les frais encourus par le déplacement avec les unités d'œuvre de prise en charge de déplacement UO_DEPL et UO_NUITEE.

02. Contexte et organisation

2.1 Présentation de la DGAMPA

La Direction Générale des Affaires Maritimes de la Pêche et de l'Aquaculture élabore et coordonne la mise en œuvre de la stratégie nationale de la mer et du littoral, réaffirmant la place de la mer au sein des politiques publiques : planification et économie maritime, flotte de commerce, pêches maritimes, aquaculture et produits de la mer, plaisance, navigation, sécurité maritime, transition écologique des navires, capitaineries de port, formation et emploi maritime.

Au sein de la sous-direction de la transformation Numérique (SDTNUM), 3 bureaux sont en charge de la gouvernance et assistance aux usagers, des produits numériques ainsi que des infrastructures, innovation numérique et data, pour proposer aux usagers des produits numériques performants et évolutifs.

Le ministère chargé de la Mer et de la Pêche est le ministère de tutelle de la DGAMPA. Il prépare et met en œuvre la politique du Gouvernement dans les domaines du développement durable, de l'environnement, du climat, de la lutte contre la pollution atmosphérique, de la protection de la nature et de la biodiversité, de l'eau, de la prévention des risques naturels et technologiques et de la sécurité industrielle, de la mer, du littoral et de la pêche maritime, de la forêt et du bois ainsi que de la promotion d'une gestion durable des ressources rares.

2.2 Missions et organisation de la Sous-Direction de la transformation Numérique (SDTNUM)

La Sous-Direction de la Transformation Numérique initie et accompagne la transformation numérique, favorise l'évolution des pratiques numériques et en assure la gouvernance. Elle veille à la mise en œuvre de la stratégie qu'elle a définie. Elle s'assure de la qualité des produits et des services et conduit l'évolution du schéma d'urbanisation, dont elle est garante, selon la logique de l'État plateforme. En lien avec l'administrateur ministériel des données, elle contribue à la valorisation du patrimoine des données de la DGAMPA et des établissements publics placés sous sa tutelle. La SDTNUM assure la veille et la prospective sur les technologies émergentes et conduit les actions d'innovation.

Les principales entités de la SDTNUM impliquées dans ou utilisatrices de prestations objet du présent marché sont :

Le Bureau de la gouvernance et appui métier (BGAU) favorise l'évolution des pratiques numériques en tenant compte de l'expérience de l'utilisateur.

Il organise la gouvernance opérationnelle des produits numériques et des référentiels en construisant et en pilotant une feuille de route de chantiers numériques incluant une programmation financière et une capacité à faire, et traitant les aspects RGPD et mise en œuvre de la politique de sécurité numérique.

Il met en place et maintient une cartographie des processus, avec l'appui des services « métier », et participe à l'élaboration de la vision urbanisée et à la stratégie d'évolution du SI ;

Il assure le pilotage bout en bout des projets numériques au profit des maîtrises d'ouvrage, en apportant un appui métier et anime les relations opérationnelles avec le SNUM du Ministère de l'Agriculture, de l'agroalimentaire et de la souveraineté alimentaire (MAASA) et la DNUM ministérielle en matière de production numérique

Il participe aux instances de représentations nationales et internationales afférentes.

Il assure la coordination de l'assistance et l'accompagnement usager par les pôles nationaux de diffusion (PND) et de la recette du système d'information de la DGAMPA et participe à la veille technologique.

Il comprend :

- Le pôle d'appui métier ;
- Le pôle gouvernance

Le Bureau des Produits Numériques (BPN) assure la conduite des opérations nécessaires à la conception, à la réalisation, à la mise en production, à l'accompagnement et au maintien des produits numériques au bénéfice des structures de la DGAMPA.

Il assure le pilotage de la réalisation des produits numériques qui lui sont confiés et le maintien en condition opérationnelle des applications.

Il assure les relations avec les prestataires informatiques attributaires des marchés de TMA / AMOE (assistance à maîtrise d'œuvre).

Il participe à la transformation du SI, pour les produits numériques de son portefeuille et à la veille technologique (état de l'art) et participe à l'élaboration et à l'amélioration des méthodologies et des outils.

Il comprend :

- Le pôle réalisation Produits numériques ;
- Le pôle livraison

Le Bureau des systèmes d'information de l'innovation et de la Data (BSIID) garantit le service d'hébergement des systèmes d'information au centre serveur du site de Saint-Malo, ainsi que le bon fonctionnement et la sécurité numérique des infrastructures du centre serveur.

Il assure la gestion et la qualité des plateformes et services de données et pilote les projets d'exploitation et de valorisation des données.

Il organise l'innovation numérique et participe à la veille technologique (état de l'art), définit les règles de conception et d'administration visant à garantir la cohérence, l'ouverture et l'interopérabilité des systèmes d'information de la DGAMPA.

Il comprend :

- Le pôle innovation / data
- Le pôle infrastructure / hébergement

03. Référentiel qualité et sécurité

3.1 PAQ et PAS

Le référentiel qualité et sécurité est défini dans deux documents distincts :

- Le **Plan d'assurance qualité PAQ**, qui devra au minimum documenter les éléments suivants :
 - Responsabilités liées au PAQ (approbation, mises à jour, procédure à suivre en cas de non-respect du PAQ...);
 - Organisation générale et responsabilités (organigramme des acteurs côté Personne Publique et côté Titulaire), comitologie : cette organisation sera chapeautée par le comité directeur du marché ;
 - Référentiel méthodologique ;
 - Référentiel technique (en fonction des stacks techniques) ;
 - Référentiel d'outillage Gestion des ressources ;
 - Modalités de fonctionnement et processus portés par le marché ;
 - Protocoles de livraison et de réception des livrables documentaires et logiciels ;
 - Suivi qualité des prestations réalisées sur le produit (définition des KPI...);
 - Indicateurs de suivi et de pilotage du projet. Ceux-ci doivent autant que possible être reliés à l'outil de *ticketing* ;
 - Outils de gestion partagée de projet ;
 - Objectifs de niveau de service ;
 - Gestion des risques en amélioration continue.
- Le **Plan d'assurance sécurité PAS**, qui devra au minimum documenter les éléments suivants :
 - Sécurité des ressources humaines ;
 - Gestion des actifs ;
 - Gestion des accès logiques ;
 - Gestion des authentifiants ;
 - Sécurité physique ;
 - Sécurité de l'exploitation des SI ;
 - Sécurité des communications ;
 - Gestion de la documentation ;
 - Contrôle et évaluation ;
 - Gestion de l'anonymisation des données ;
 - Sécurité des développements ;

- Maintenance des SI ;
- Gestion de la continuité d'activité ;
- Mise à jour des systèmes logiciels ;
- Gestion des situations de télétravail ou d'astreinte.

Ces documents seront rédigés au lancement du marché (unité d'œuvre UO_LANCEMENT) par le titulaire.

3.2 Réglementation

Les documents suivants (liste non exhaustive) accessibles à partir du site de l'Agence Nationale de Sécurité des Systèmes d'information (ANSSI), dans leur version à leur date de publication, font référence :

- Arrêté du 30 mars 2021 portant approbation du cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication CCAG TIC
<https://www.legifrance.gouv.fr/download/pdf?id=ldfuwxkMUjizT4kHO04ncYPCIFRafx3LLgujSD-i24w=>
- L'instruction interministérielle N°901 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR)
<https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-interministerielle-n-901/>
- L'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale <https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministerielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/>
- La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)
<https://www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformatons/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/>
- Le référentiel général de sécurité (RGS V2)
<https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/>
- Les recommandations et bonnes pratiques de l'ANSSI :
https://cyber.gouv.fr/publications?field_type_de_publication_target_id%5B934%5D=934

3.3 Cadre normatif et exigences de sécurité

Le **Responsable de la Sécurité des Système d'Information** (RSSI) de la SDTNUM est en charge de la mise en application de la Politique SSI du pôle ministériel.

Au titre du marché, le titulaire s'engage à réaliser sa prestation conformément aux exigences de sécurité et de qualité qui découlent de la PSSI de l'État, du Référentiel Général de sécurité (RGS) et des référentiels RGI et RGAA.

Le personnel du titulaire devra faire acte d'accuser réception individuellement de la PSSI du Ministère. Le personnel du titulaire qui interviendra sur le SI du pôle ministériel devra en outre faire acte d'accuser réception individuellement de la charte d'usage des systèmes et services informatiques du ministère, telle que mise à disposition par la Personne Publique.

Cette charte fixe notamment :

- Les règles de sécurité et de confidentialité des systèmes et données de l'administration.
- Les modalités d'accès, d'utilisation et de partage des ressources informatiques mises à disposition.
- Les obligations relatives à la protection des données personnelles et des données de santé.

Les interdictions, notamment concernant l'installation de logiciels non autorisés, le partage de mots de passe ou le transfert de données sur des supports non sécurisés.

Le titulaire est responsable de la sensibilisation et du contrôle de son personnel au respect de cette charte.

Toute violation de la charte pourra entraîner des sanctions prévues au CCAP, et le bénéficiaire se réserve le droit de suspendre l'accès aux systèmes concernés tant que la situation n'est pas régularisée.

Ces documents lui seront adressés individuellement via un courriel. Le titulaire s'assurera que son personnel a fait acte d'accuser de réception. Dans l'éventualité où pour exercer sa mission le personnel du titulaire aurait besoin de disposer de privilèges administrateurs sur un poste de travail de l'administration, il devra justifier sa demande et s'engager à respecter les règles précisées dans le document de dérogation à la charte d'utilisation des ressources informatiques et des moyens de télécommunication et signer le formulaire correspondant.

Dans le cadre des prestations de TMA, le titulaire devra être très vigilant sur la sécurité applicative en identifiant les risques sécurité les plus critiques qui sont détaillés notamment dans les travaux de l'OWASP (Open Web Application Security Project) et devra respecter les principes énoncés dans les différents guides de l'OWASP ainsi que les règles et normes de développement de la SDTNUM.

De plus, en complément des exigences décrites au paragraphe précédent, la SDTNUM respecte les règles définies dans les référentiels interministériels suivants :

- Le référentiel Agilité et sécurité numérique de l'ANSSI et la DINUM
<https://www.ssi.gouv.fr/guide/agilite-et-securite-numeriques-methode-et-outils-a-lusage-des-equipes-projet/>
- Le référentiel des règles d'interopérabilité (RGI)
<https://www.numerique.gouv.fr/publications/interoperabilite/>
- Le référentiel des règles d'ergonomie, de charte graphique et d'accessibilité RGAA
<https://www.numerique.gouv.fr/publications/rgaa-accessibilite/>
- Le référentiel général d'écoconception de services numériques RGESN
<https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/>

Il est attendu du titulaire qu'il mette en place des mesures organisationnelles et techniques pour contrôler la qualité et la sécurité de ses prestations. A la demande de la SDTNUM, celui-ci est tenu de produire les justifications ou rapport montrant les investigations et les contrôles réalisés.

Le personnel du titulaire n'est pas autorisé à faire usage des matériels et des logiciels du pôle ministériel en dehors du cadre strict de sa mission.

L'organisation, la démarche et les dispositifs techniques mis en place par le titulaire pour prendre en compte la sécurité au sens des normes ISO27001 et ISO27002 sur ses centres de service et sur l'ensemble des prestations du marché sont fixées dans son offre.

Par ailleurs, le titulaire s'engage à respecter l'ensemble des exigences de sécurité relatives aux développements informatiques réalisés à partir de ses locaux et nécessitant des accès sur les plateformes de la SDTNUM. En l'espèce, sont exposées dans son offre l'organisation générale de sa politique de sécurité (PAS) et plus particulièrement les mesures qui s'appliquent à ses centres de service ainsi que les caractéristiques de leur sécurité logique (gestion des habilitations, antivirus, ...) et physique (sécurité de l'environnement, contrôles d'accès, ...).

Les accès au SI de la DGAMPA et du ministère et les échanges devront s'effectuer dans le respect des procédures de la SDTNUM qui s'appuient sur les politiques en vigueur (PSSI Ministère, Norme ISO 27001 : 2013, Norme ISO 27002 : 2013).

En cas de modification des règles de sécurité d'accès, la SDTNUM communique par mail les nouvelles règles avec un préavis d'un mois minimum au titulaire. Ce dernier doit se mettre en conformité avec les nouvelles règles, sans que les évolutions des règles de sécurité puissent donner lieu à ajustement tarifaire ; l'évolution des règles de sécurité ne peut en aucun cas motiver des limitations des engagements du titulaire, de façon temporaire ou définitive, sauf accord exprès préalable de la part de la SDTNUM.

En cas de manquement du titulaire, l'Administration se réserve le droit de ne pas valider les prestations concernées jusqu'à résolution complète par le titulaire des problèmes de sécurité identifiés (l'allongement des délais de la prestation pouvant induire des pénalités telles que prévues dans les unités d'œuvre commandées). En cas de persistance des problèmes ou de manquements répétés, l'Administration se réserve le droit de dénoncer le présent marché.

3.4 Communication des incidents de sécurité

Dans l'éventualité où le Titulaire constaterait ou suspecterait un incident de sécurité affectant l'un de ses centres de service ou les prestations réalisées pour la SDTNUM, il est tenu d'en informer par tout moyen disponible et sans délai le service de sécurité des systèmes d'information du Ministère.

3.5 Publication de vulnérabilité – Attaques – Actions de prévention

Dans le cadre du maintien optimum et opérationnel de la sécurité, il est envisagé, lors de la publication de vulnérabilités affectant le socle technique, les applications ou les bases de données de la DGAMPA, ou lors d'éventuelles attaques ou d'actions de prévention, la mise en œuvre d'un ensemble de mesures spécifiques (par exemple : application de correctifs techniques ou de sécurité, mesures conservatoires...).

Il est alors demandé au titulaire de prendre les mesures nécessaires à cette mise en œuvre. Ces mesures n'ont pas vocation à être optionnelles, mais recouvrent un caractère obligatoire. Si le titulaire refuse ces mesures dans les délais impartis, il doit apporter à la SDTNUM la preuve de cette impossibilité technique et en exposer les conséquences induites.

Dans le cas où l'argumentaire fait par le titulaire de son impossibilité d'action n'est pas validé par la SDTNUM, le titulaire a obligation de réaliser cette mise en œuvre dans les délais impartis (délais définis dans les unités d'œuvre liées à l'intervention demandée).

Dans le cas où la preuve est faite par le titulaire de son impossibilité d'action, il lui est demandé, soit lors d'une prochaine mise en œuvre opérationnelle, soit lors d'une maintenance programmée, d'effectuer les travaux demandés. Dans le cas où la dégradation de service est jugée acceptable par la SDTNUM, il pourra être demandé la mise en œuvre d'une partie seulement de ces corrections.

En tout état de cause, lors de ces différents travaux, le titulaire se garantit par la réalisation d'une sauvegarde permettant un retour arrière pour tout problème bloquant rencontré.

3.6 Audit

La SDTNUM peut à tout moment engager des audits sur les prestations et les résultats produits dont des audits de la qualité et de la sécurité du code. Le titulaire s'engage à mettre à disposition de la SDTNUM – ou à tout intervenant mandaté par elle – l'ensemble des éléments permettant les opérations d'audits

Le titulaire s'engage, dans ce cadre, à faire diligence et ne saurait, sans exception dûment motivée, différer la mise à disposition des éléments nécessaires aux opérations d'audit, au-delà de 3 jours ouvrés. Le titulaire doit laisser libre accès à l'ensemble de ses productions et, en général, faciliter les tâches de l'auditeur.

Les conclusions de l'audit sont communiquées le cas échéant au titulaire sur décision de la SDTNUM.

Si un rapport d'audit fait apparaître des anomalies et/ou des non-conformités, le titulaire met en œuvre les mesures correctives nécessaires dans un délai convenu avec la SDTNUM à compter de la notification des insuffisances par la SDTNUM et en application des conditions de prise en charge et de garantie des développements informatiques réalisés dans le cadre du marché.

3.7 Cadre technique

Le titulaire pourra utiliser les outils de développements, les outils collaboratifs, et les outils techniques de la SDTNUM ou ses propres outils.

Par contre, les livrables attendus (code source, documentation, ...) devront être versés sur la forge *Gitlab* du pôle ministériel et les outils collaboratifs de la SDTNUM.

Le titulaire doit veiller à réaliser ses interventions, quelles que soient leur nature, en veillant à :

- L'adaptabilité,
- La robustesse,
- La réutilisabilité,

- La maintenabilité,
- La qualité,
- La sécurité,
- L'accessibilité,
- La mobilité (le « *multi-device* »)

des applications conformément aux exigences définies au chapitre "Cadre normatif et exigences de sécurité".

3.8 Analyse statique de la qualité et de la sécurité du code

Le code (programme) devra respecter les règles des bonnes pratiques en programmation. Notamment le titulaire pourra utiliser des outils comme *Sonarqube*, *SonarLite*, *Gitlab*, etc.

Certains contrôles en ce sens, dont aura été informé le titulaire au préalable, pourront être effectués par l'ordonnateur et pourront être cause de rejet du livrable concerné.

Au démarrage du marché, la SDTNUM et le Titulaire se mettront d'accord sur la mise en place des outils d'analyse et les critères de recevabilité.

3.9 Résorption de la dette technique

La résorption de la dette technique, la qualité et la sécurité des applications sont un enjeu pour la SDTNUM.

Au lancement du marché, le Titulaire relèvera les indicateurs liés à l'analyse et à la sécurité du code des applications de son périmètre : les notes, le nombre de vulnérabilité par niveau de criticité, le nombre de mauvaises pratiques, la dette technique, etc.

Pour les applications présentant une dette technique héritée des précédents prestataires, si nécessaire (à indiquer dans le PAQ), le titulaire proposera un plan d'action visant à réduire cette dernière et à améliorer les notes des applications dont il assure la maintenance. Un point de situation et un bilan seront réalisés lors des Comités de pilotage du marché.

Dans le cadre de ses opérations de maintenance, il est attendu du titulaire qu'il laisse les sources conformes à l'état de l'art. En cas d'accroissement de la dette technique suite à ses interventions, le titulaire veillera à revenir au seuil antérieur en réalisant les opérations nécessaires sans surcoût (sauf s'il est acté avec le bénéficiaire que l'application est en fin de vie).

3.10 Conditions spécifiques liées à l'usage de l'Intelligence Artificielle

Le prestataire pourra recourir à des outils d'intelligence artificielle (IA) dans le cadre de l'exécution des prestations. Ces outils doivent respecter les exigences suivantes :

- Respect de la confidentialité et de la sécurité des données du maître d'ouvrage,
- Conformité avec la réglementation en vigueur,
- Garantie d'absence d'atteinte aux droits de tiers.

Le prestataire s'engage à informer préalablement le maître d'ouvrage de tout recours significatif à des outils d'IA et à fournir un rapport annuel décrivant leur usage.

3.11 Licences logicielles et dépendances

Le prestataire garantit que tous les logiciels et composants utilisés dans le cadre du présent marché sont dûment licenciés et que leur utilisation est conforme aux droits d'exploitation concédés au maître d'ouvrage.

Toutes les dépendances logicielles tierces doivent être déclarées avec leurs conditions de licence. Le prestataire s'assure que ces licences permettent l'usage prévu, sans frais additionnels non prévus dans le marché.

Dans le cas de logiciels open source, le prestataire vérifie la compatibilité des licences avec l'utilisation envisagée et informe le maître d'ouvrage de leurs impacts éventuels.

04. Modalités d'exécution du marché

4.1 Principes généraux de gouvernance du marché

Le pilotage contractuel du marché doit permettre de disposer d'une gouvernance côté Titulaire pour encadrer toutes les prestations du marché. Cette gouvernance se caractérise par des activités récurrentes et transverses pendant l'exécution du marché, pour assurer la coordination globale des différentes prestations, garantir la cohérence des différents livrables et gérer les processus qualité.

La gouvernance du marché est décrite au point 4.2. « Suivi contractuel et pilotage général » précisé ci-dessous.

Le coût du pilotage contractuel est inclus dans le coût des UO et ne génère pas de facturation complémentaire.

Une plateforme de travail collaboratif mise à disposition par la personne publique sera utilisée pour gérer l'ensemble des productions relatives aux instances définies ci-dessous :

- Ordre du jour.
- Support de présentation.
- Compte rendu des instances.

Le titulaire est en charge de la production de ces documents sous couvert de la validation par la personne publique.

Les participants aux instances peuvent décider d'inviter tout participant qualifié, en fonction de l'ordre du jour. Chaque partie en informe au préalable l'autre partie.

4.2 Suivi contractuel et pilotage général

Les instances suivantes sont mises en place pour gérer le management des prestations :

- Comité de pilotage du marché semestriel
- Comité technique du marché trimestriel
- Comité de suivi d'un portefeuille de produits numériques mensuel

Instance	Périmètre et fréquence	Objectifs principaux	Participants
Comité de pilotage du marché	Ce comité se réunit deux fois par an, à distance.	<p>Valider le PAQ et gérer ses évolutions</p> <p>Suivre le déroulement de l'exécution du marché selon les indicateurs de pilotage définis dans le PAQ du marché :</p> <ul style="list-style-type: none"> • Suivre l'évolution des portefeuilles, des plans de charge • Suivre la qualité des prestations et la satisfaction de l'administration • Arbitrer : Analyser les problèmes d'exécution rencontrés non résolus dans les autres instances, définir les solutions à apporter. • Capitaliser : Identifier les éléments à mutualiser, les sujets à porter par le comité technique 	<p>Titulaire :</p> <p>Représentant de la direction du titulaire</p> <p>Directeur de projet</p> <p>Directeur technique du marché</p> <p>Administration :</p> <p>Chef(fe)s de Bureau</p> <p>Coordinateur du marché</p> <p>Directeurs de produits</p>
Comité technique du marché	Cette instance se réunit à l'initialisation du marché et autant que de besoin – par défaut 4 fois par an, à distance.	<p>Vérifier la bonne prise en compte des exigences techniques définies par l'administration</p> <p>Suivre l'usage par le titulaire des référentiels technique et méthodologique de l'administration et leurs évolutions</p> <p>Identifier et suivre les évolutions à mettre en œuvre : outils et leurs paramétrages, composants, méthodes, bonnes pratiques</p> <p>Capitaliser pour s'assurer qu'une solution mise en œuvre pour un département peut être utilisée à moindre coût pour un autre département.</p>	<p>Titulaire :</p> <p>Responsable technique</p> <p>Directeurs de projet des différents portefeuilles de produits</p> <p>Experts techniques</p> <p>Administration :</p> <p>Coordinateur du marché</p> <p>Experts sécurité, du génie logiciel de l'offre d'hébergement...</p> <p>Chefs de bureau et/ou chefs ou directeurs de produit éventuellement</p>

Instance	Périmètre et fréquence	Objectifs principaux	Participants
Comité de management d'un portefeuille de produits	<p>Ce comité se réunit environ tous les mois selon l'activité du département concerné, à distance ou dans les locaux du département.</p> <p>En cas de manquement du titulaire, l'Administration se réserve le droit de ne pas valider les prestations concernées jusqu'à résolution complète par le titulaire des problèmes de sécurité identifiés (l'allongement des délais de la prestation pouvant induire des pénalités telles que prévues dans les unités d'œuvre commandées). En cas de manquements répétés, l'Administration se réserve le droit de dénoncer le présent marché.</p>	<p>Valider le PAQ de maintenance des SI du portefeuille et gérer ses évolutions</p> <p>Suivre le déroulement de l'exécution du portefeuille selon les indicateurs de pilotage définis dans le PAQ correspondant.</p> <p>Suivre le déroulement de l'exécution du portefeuille selon les indicateurs de pilotage définis dans le PAQ correspondant :</p> <ul style="list-style-type: none"> Suivre l'évolution du portefeuille SI, des plans de charge, des ressources affectées, de l'exécution budgétaire, valeur apportée Partager les enjeux métier, suivre globalement l'avancement des projets, des risques et des plans actions associés, identifier les besoins en ressources spécifiques Arbitrer : Analyser les problèmes d'exécution rencontrés, définir les solutions à apporter Suivre la mise en œuvre des exigences techniques, contribuer à la capitalisation. 	<p>Titulaire :</p> <p>Représentant du titulaire</p> <p>Directeur de projet du portefeuille de produits</p> <p>Administration :</p> <p>Chef(fe)s de Bureau</p> <p>Directeurs de produits et/ou Chefs de produits</p>

4.3 Instances de suivi opérationnel des prestations

Les instances suivantes sont mises en place pour le suivi opérationnel des prestations autant que de besoin :

1. Comité de produit
2. Réunion projet/produit

Instance	Périmètre et fréquence	Objectifs principaux	Participants
Comité produit	Un comité titulaire-administration peut être mis en place pour un SI	<p>Suivre le déroulement des projets : gestion des plans d'actions, gestion des risques, gestion des ressources, analyse des impacts des changements d'exigence</p> <p>Préparer les arbitrages pour le métier (coûts/délais)</p>	<p>Titulaire :</p> <p>Directeur de projet du portefeuille</p> <p>Chefs de projet concernés</p>

Instance	Périmètre et fréquence	Objectifs principaux	Participants
	donné. Il se réunit selon le contexte	Instruire les problèmes rencontrés	Experts Administration : Directeurs de produit et Chefs de produit concerné(s)
Réunion projet/produit	Des réunions peuvent être organisées entre les chefs de projets titulaire et administration autant que de besoin. Elles ont lieu selon le contexte.	Préparer les commandes Suivre le déroulement des prestations	Titulaire : Chef(s) de projet concerné(s) Administration : Directeurs de produit et Chef(s) de projet/produit concerné(s)

4.4 Processus relatif à la réception des livrables

Les opérations de constatation, de vérification et d'admission sont effectuées dans les conditions stipulées au CCAG/TIC :

- Tout avis de rejet est motivé et formalisé par écrit au prestataire.
- Les opérations sont effectuées par la Personne Publique ou par un tiers désigné à cet effet.

Les opérations de vérification quantitative et qualitative des prestations sont menées dans les locaux de l'acheteur et/ou dans ceux du Titulaire.

Les décisions de l'acheteur sont conformes au CCAG/TIC :

- L'admission est la décision, prise après vérifications, par laquelle l'acheteur reconnaît la conformité des prestations aux stipulations du marché. La décision d'admission vaut constatation de service fait et constitue le point de départ des délais de garantie.
- L'ajournement est la décision prise par l'acheteur qui estime que les prestations pourraient être admises moyennant des corrections à opérer par le Titulaire.
- La réfaction est la décision prise par l'acheteur de réduire le montant des prestations à verser au Titulaire, lorsque les prestations ne satisfont pas entièrement aux prescriptions du marché, mais qu'elles peuvent être admises en l'état.
- Le rejet est la décision prise par l'acheteur qui estime que les prestations ne peuvent être admises, même après ajournement ou avec réfaction.

Les modalités de mise en œuvre des avances et des acomptes sont conformes au CCAG/TIC.

4.5 Admission des livrables conditionnée par une réception, suivie d'une vérification d'aptitude (VA) et une vérification du service régulier (VSR)

Les prestations suivantes sont admises par réception, vérification d'aptitude (VA) (sprint n+1 en mode agile) et vérification de service régulier (VSR) (sprint n+2 en mode agile) :

- Réalisation des composants (UO_REA) ;
- Reprise et mise en qualité des données (UO_REPRISE) ;
- Itération de développement (UO_IT) ;
- Maintenance adaptative (UO_MJCA, UO_MCA, UO_MBD).

L'acheteur prononce (admission) :

- La réception, si toutes les anomalies bloquantes ont été corrigées ;
- La fin de VA, si toutes les anomalies majeures ont été corrigées ;
- La fin de VSR, si toutes les anomalies mineures ont été corrigées.

Dans le cas contraire, l'acheteur peut prendre les décisions suivantes en fin de réception, de VA ou de VSR :

- Ajournement n'entraînant pas une suspension des pénalités de retard prévues dans l'article 6.13.1 du CCAP ;
- Réfaction ;
- Rejet n'entraînant pas une suspension des pénalités de retard prévues dans l'article 6.13.1 du CCAP et, dans ce cas, les livrables ne sont pas livrés et la prestation n'est pas payée. Celle-ci doit être recommencée.

La décision est formalisée par l'émission d'un PV de réception, de fin de VA ou de fin de VSR.

La durée des phases de vérification est définie dans les unités d'œuvre concernées.

Le paiement des prestations intervient à hauteur de :

- 70% à la réception ;
- 15% à la fin de la VA ;
- 15% à la fin de la VSR.

4.6 Admission conditionnée par une réception suivie d'une validation documentaire

Les prestations suivantes sont admises par réception et validation :

- Lancement du marché (UO_LANCEMENT) ;
- Initialisation et Prise en charge d'une nouvelle application (UO_PCHA) ;
- Mise en place d'un POC technique (UO_POC) ;
- Étude d'impact (UO_EIMPT et UO_EIMPF) ;
- Spécifications fonctionnelles détaillées (UO_SFD) ;
- Conception fonctionnelle (UO_CONCF) ;
- Rétro-documentation (UO_RETDOC) ;
- Conception technique (UO_DAT) ;
- Cadrage d'une version en agile/DevOps/produit (UO_CADAG) ;
- Audit technique ou audit de code (hors sécurité) (UO_AUDIT) ;
- Appui Product Owner (UO_APO) ;
- Appui Méthode (UO_AM) ;
- UI/UX Ergonomie (UO_UX) ;
- Appui à l'intégration (UO_INTEGR) ;
- Expertise technique ponctuelle (UO_EXP_ARCHI, UO_EXP_DATA, UO_EXP_SECU, UO_EXP_GEO, UO_EXP_URBA) ;
- Transfert de compétence sur un produit (UO_PREP_TDC, UO_TDC) ;
- Réversibilité/transférabilité sur une application (UO_REVERS).

La durée des phases de vérification est définie dans les unités d'œuvre.

Le paiement de ces prestations intervient à hauteur de :

- 70% à la réception
- 30% à la fin de la validation

Pour les prestations qui délivrent des produits documentaires, les opérations de vérification sont réalisées après la livraison.

Elles prennent d'abord la forme d'une réception (une présentation formelle du (des) livrable(s) peut être réalisée à la demande de la Personne Publique), puis d'une validation qui ont pour but de constater que les produits documentaires sont tous livrés et qu'ils sont conformes et exhaustifs par rapport à la commande.

La Personne Publique prononce donc (admission) :

- La réception, si toutes les anomalies documentaires critiques ont été corrigées ;
- La fin de validation, si toutes les anomalies majeures et mineures ont été corrigées.

Dans le cas contraire, l'acheteur peut prendre les décisions suivantes :

- Ajournement n'entraînant pas une suspension des pénalités de retard prévues dans l'article 6.13.1 du CCAP ;
- Réfaction ;
- Rejet n'entraînant pas une suspension des pénalités de retard prévues dans l'article 6.13.1 du CCAP et, dans ce cas, les livrables ne sont pas livrés et la prestation n'est pas payée. Celle-ci doit être recommencée.

La décision est formalisée par l'émission d'un PV de réception ou de fin de validation.

4.7 Admission conditionnée par une constatation mensualisée

Les prestations suivantes sont admises par une constatation mensualisée :

- Maintenance corrective et préventive d'un produit numérique (UO_MCORR) ;

Le paiement de ces prestations intervient mensuellement, au *prorata temporis*.

L'acheteur vérifie chaque mois la conformité des fournitures ou des services exécutés avec les spécifications du bon de commande et procède à son admission par la constatation du service fait. A l'issue des opérations de vérification, l'acheteur peut prendre les décisions suivantes :

- Admission ;
- Ajournement n'entraînant pas une suspension des pénalités de retard prévues dans l'article 6.13.1 du CCAP ;
- Réfaction ;
- Rejet n'entraînant pas une suspension des pénalités de retard prévues dans l'article 6.13.1 du CCAP et, dans ce cas, les livrables ne sont pas livrés et la prestation n'est pas payée. Celle-ci doit être recommencée.

La décision est formalisée par l'émission d'un constat de service fait.

4.8 Portage d'expertise indépendante

En cours de marché, certains produits numériques peuvent nécessiter l'appel à des expertises rares, sur une technologie ancienne ou bien sur un outillage ou progiciel spécifique, non prévisibles au démarrage du marché.

Dans ce cas, l'Administration peut demander au titulaire d'assurer le portage d'un(e) expert(e) indépendant(e) sélectionné(e) par l'Administration.

Le portage consiste en une relation tripartite entre le titulaire, l'expert(e) indépendant(e) et le bénéficiaire de l'Administration. Un contrat est établi entre le titulaire et l'expert(e) indépendant(e), en direct ou via une société de portage (déclarée comme sous-traitante), tandis que le contrat de prestation du présent marché est conclu entre le titulaire et l'Administration pour qui l'expert(e) indépendant(e) effectue la prestation.

A noter :

1/ que l'Administration ne contractualise qu'avec le titulaire du présent marché et non avec les experts indépendants ou une éventuelle société de portage ;

2/ que le coût journalier de l'expert indépendant doit rester inférieur ou égal au TJM d'un intervenant du titulaire pour un profil similaire, sauf démonstration par le titulaire de l'impossibilité de trouver des profils à un coût journalier inférieur ou égal aux TJM du marché.

Le titulaire pourra appliquer un taux de portage.

Le taux de portage est un pourcentage du coût de l'expert(e) indépendant(e) et qui vient s'ajouter au coût d'intervention de l'expert indépendant.

Le taux de portage est fixe quelle que soit l'expertise pour toute la durée du marché ; il est indiqué dans l'annexe 1, BPU, à l'acte d'engagement.

Une fois l'intervenant choisi et la validation finale effectuée par le bénéficiaire, le Titulaire établit un devis correspondant au coût de l'expert indépendant multiplié par le coefficient de portage. La commande est passée par l'Administration, sur la base de ce devis, exclusivement au titulaire.

4.9 Réversibilité et transférabilité

Les opérations de réversibilité et de transférabilité sont effectuées dans les conditions stipulées à l'article 38.4 du CCAG/TIC du 30 mars 2021, le délai de transition étant de 6 mois.

4.10 Gestion du turn-over

Dans tous les cas, le turn-over en cours de prestation doit faire l'objet d'un biseau de transfert de compétences de cinq jours ouvrés au minimum, entre la ressource sortante et la ressource entrante.

Le coût de ce biseau est à la charge du Titulaire si le turn-over lui est imputable.

PROCEDURE DE TURN-OVER IMPUTABLE AU TITULAIRE

Dans le cas du *destaffing* d'une ressource du Titulaire (démission, changement d'activité...), la procédure de turn-over est la suivante :

1) Le Titulaire avertit par écrit la Personne Publique du départ d'un intervenant, le plus tôt possible et au minimum trente jours ouvrés avant la date de départ souhaitée ; le non-respect de ce délai fait encourir au Titulaire la pénalité prévue à l'article 6.13.2 du CCAP.

2) Le Titulaire communique par écrit le CV du ou des candidats au minimum quinze jours ouvrés avant la date de départ de l'intervenant ; le non-respect de ce délai fait encourir au Titulaire la pénalité prévue à l'article 6.13.2 du CCAP.

3) La Personne Publique dispose d'un délai de cinq jours ouvrés pour valider l'équivalence de compétences sur la base du CV fourni :

- Si l'équivalence n'est pas constatée ou si les compétences de l'intervenant proposé ne sont pas satisfaisantes, la Personne Publique le notifie par écrit au Titulaire qui reprend la procédure au point 2. En cas d'un nouvel échec, la Personne Publique peut appliquer la pénalité prévue à l'article 6.13.2 du CCAP.
- Si l'équivalence est constatée et si les compétences de l'intervenant proposé sont satisfaisantes, la Personne Publique le notifie par écrit au Titulaire et organise, si besoin, un entretien afin d'évaluer précisément les compétences et la séniorité de l'intervenant sur la mission qu'il doit assurer.

4) Tout remplacement est considéré comme définitivement accepté si l'équivalence de compétences est constatée par la Personne Publique dans un délai d'un mois à compter de la prise de fonction.

5) Dans le cas contraire, la Personne Publique peut récuser le remplaçant. La procédure reprend alors au point 2 et le Titulaire dispose de cinq jours ouvrés pour désigner un autre remplaçant et en informer la Personne Publique.

- À défaut de désignation, ou si ce remplaçant est récusé dans le délai d'un mois, la Personne Publique peut appliquer la pénalité prévue à l'article 6.13.2 du CCAP.

PROCEDURE DE TURN-OVER IMPUTABLE A LA PERSONNE PUBLIQUE OU RECHERCHE DE PROFIL

Dans le cas du *destaffing* d'une ressource défaillante à la demande de la Personne Publique, ou de recherche d'un nouveau profil, la procédure à suivre est décrite ci-après :

1) La Personne Publique notifie par écrit au Titulaire sa demande de remplacement d'un intervenant ou de recherche d'un nouveau profil, le plus tôt possible et au minimum trente jours ouvrés avant la date de prise de poste souhaitée.

2) Le Titulaire communique par écrit le CV du ou des candidats, au maximum quinze jours ouvrés après la demande ; le non-respect de ce délai fait encourir au Titulaire la pénalité prévue à l'article 6.13.2 du CCAP.

3) La Personne Publique dispose d'un délai de cinq jours ouvrés pour valider les compétences sur la base du CV fourni :

- Si les compétences de l'intervenant proposé ne sont pas satisfaisantes, la Personne Publique le notifie par écrit au Titulaire qui reprend la procédure au point 2. En cas d'un nouvel échec, la Personne Publique peut appliquer la pénalité prévue à l'article 6.13.2 du CCAP.
- Si les compétences de l'intervenant proposé sont satisfaisantes, la Personne Publique le notifie par écrit au Titulaire et organise si besoin un entretien avec l'intervenant proposé afin d'évaluer précisément les compétences et la séniorité de l'intervenant sur la mission qu'il doit assurer.

4) À la suite de l'entretien, la Personne Publique dispose d'un délai de cinq jours ouvrés pour notifier par écrit la validation de la candidature. En cas de refus, le Titulaire reprend la

procédure au point 2. En cas de nouvel échec, la Personne Publique peut appliquer la pénalité prévue à l'article 6.13.2 du CCAP.

5) Tout remplacement est considéré comme définitivement accepté si l'équivalence de compétences est constatée par la Personne Publique dans un délai d'un mois à compter de la prise de fonction.

6) Dans le cas contraire, la Personne Publique peut récuser l'intervenant. La procédure reprend alors au point 2 et le Titulaire dispose de cinq jours ouvrés pour désigner un autre remplaçant et en informer la Personne Publique.

7) À défaut de désignation, ou si ce remplaçant est récusé dans le délai d'un mois, la Personne Publique peut appliquer la pénalité prévue à l'article 6.13.2 du CCAP.

4.11 Formation et qualification des ressources proposées par le Titulaire

Le Titulaire s'engage :

- Sur les compétences des profils proposés, en conformité avec le niveau de séniorité et les compétences attendus pour les intervenants ;
- À effectuer toutes les actions de formation nécessaires pour mettre au niveau requis ou pour maintenir le niveau de compétence de son personnel pendant la durée du marché ;
- À ce que tout nouvel arrivant ait reçu, avant le démarrage des prestations, une information à sa charge sur les clauses du marché, les méthodes, techniques et outils utilisés ;
- En cas de remplacement, à fournir les efforts nécessaires pour amener tout nouvel intervenant au niveau de compétence requis pour les missions qu'il doit assurer, en pratiquant une période de recouvrement suffisante et aux frais du Titulaire.

Ces engagements impliquent que le Titulaire veille à ce que l'équipe en place soit la plus stable possible et que tout turn-over soit anticipé pour minimiser l'impact sur la production et maintenir le niveau de service défini sur le produit.

4.12 Les horaires de travail

Les prestations sont exécutées dans le cadre horaire défini par la réglementation en vigueur au sein de l'établissement de la Personne Publique.

En cas d'indisponibilité des intervenants pour des raisons prévisibles, celles-ci sont à signaler à la Personne Publique dans un délai de prévenance de 15 jours.

05. Description des prestations attendues

5.1 Les prestations et unités d'œuvre du marché

LES TYPES DE PRESTATIONS

Les prestations sont de plusieurs natures :

- Initialisation et réversibilité ;
- Maintenance corrective et préventive ;
- Maintenance évolutive et adaptative ;
- Expertise et accompagnement ;
- Autres prestations transverses.

Elles reposent sur des unités d'œuvre.

Une **unité d'œuvre (UO)** est constituée par un ensemble de tâches assorti d'une obligation de résultat et d'un délai d'exécution fixé, dans un cadre financier forfaitaire ou capacitaire.

Chaque unité d'œuvre définit notamment :

- Les objectifs attendus,
- Les tâches à réaliser,
- Les éléments mis à disposition du prestataire,
- Les livrables attendus,
- Les niveaux de complexité,
- La durée de l'UO, ses délais d'exécution, les pénalités applicables en cas de retard,
- Éventuellement la périodicité des commandes.

Les UO sont décrites **en annexe 1**.

LA CHARGE DE PILOTAGE

La part de pilotage est comprise dans le prix de l'UO proposé par le Titulaire.

LA DUREE EVOQUEE DANS LES UO

La durée moyenne d'une réunion de travail est de 2h et celle d'un atelier est de 3h à 4h.
Pour les UO dimensionnées sur une journée, la journée standard correspond à 7 heures.

5.2 Outillage de gestion

L'enregistrement et le suivi des demandes (support, anomalies, incidents, évolution) se font dans un outil fourni par le titulaire ou par l'administration. Le choix se fait lors de l'initialisation.

Cet outil doit permettre le suivi des demandes par la Personne Publique et s'intégrer au *reporting* du titulaire.

Les demandes d'évolution sur un produit numérique sont gérées dans le *backlog* d'évolutions du produit.

Les anomalies détectées sur un produit numérique sont gérées dans le *backlog* d'anomalies du produit.

5.3 Notion d'anomalie

01) ANOMALIE DE PROJET

Une anomalie de projet correspond à toute non-conformité aux spécifications constatée par la Personne Publique.

Les anomalies sont signalées au Titulaire via l'outil de gestion.

Les anomalies de projet sont classées en trois niveaux de gravité en fonction de leur incidence sur le pipeline de développement, intégration, recette et déploiement du produit :

- **Anomalie bloquante** : l'anomalie correspond à une non-conformité aux spécifications du *backlog* ; elle rend impossible l'intégration et le déploiement de la release du produit et/ou bloque l'ensemble du processus de recette ;
- **Anomalie majeure** : l'anomalie correspond à une non-conformité aux spécifications du *backlog* ; elle ne permet pas d'intégrer et de déployer la totalité de la release du produit et/ou bloque une partie du processus de recette ;
- **Anomalie mineure** : toute autre anomalie non bloquante ou non majeure.

ANOMALIE DOCUMENTAIRE

Toute documentation non conforme doit être corrigée par le titulaire du marché au même titre qu'une anomalie de projet. Les anomalies sont signalées au Titulaire via l'outil de gestion.

Les anomalies de documentation sont classées en trois niveaux de gravité :

- **Anomalie critique** : tout élément documentaire ne permettant pas d'intégrer et de déployer un produit et/ou qui rend l'application inexploitable et/ou qui génère des dégradations voire des pertes de données ;

- **Anomalie majeure** : tout élément documentaire ne correspondant pas au produit numérique cible (pour la documentation fonctionnelle, technique et métier), et plus largement, dont les informations sont incomplètes ou fausses ;
- **Anomalie mineure** : tout élément documentaire contenant des fautes d'orthographe et ne respectant pas les conventions de forme ou de structure.

ANOMALIE DE FONCTIONNEMENT

Une anomalie de fonctionnement désigne toute panne, tout incident, tout blocage, tout dysfonctionnement ou toute dégradation de performances constatés sur tout ou partie d'un service applicatif à la charge du Titulaire dans le cadre du marché.

Les anomalies sont signalées au Titulaire via l'outil de gestion.

Les anomalies de fonctionnement sont classées en trois niveaux de gravité selon leur incidence sur l'activité des utilisateurs :

- **Anomalie bloquante** : panne, incident ou dysfonctionnement qui empêche l'utilisation de tout ou partie du service applicatif, et pour lequel aucune procédure de contournement ne peut être mise en place ;
- **Anomalie majeure** : panne, incident ou dysfonctionnement qui empêche l'utilisation de tout ou partie du service applicatif, tout en permettant l'obtention du résultat attendu par une procédure de contournement simple et acceptée par la Personne Publique. À défaut d'une procédure de contournement acceptée, cette anomalie est considérée comme bloquante ;
- **Anomalie mineure** : panne, incident ou dysfonctionnement qui a un faible impact sur l'usage du service applicatif, caractérisée par une simple gêne de l'utilisateur.

DELAI DE CORRECTION DES ANOMALIES

Les anomalies de fonctionnement sont prises en charge selon des délais définis dans les unités d'œuvre, en fonction du niveau de service attendu.

En cas de non-respect des délais, les pénalités décrites dans les unités d'œuvre sont applicables.

Dans le cas où les unités d'œuvre ne précisent pas de pénalités, l'article 14 du CCAG TIC du 30 mars 2021 s'applique.

Si le produit fait l'objet de maintenance évolutive, les anomalies de fonctionnement hors garantie sont introduites dans le *backlog* d'évolutions et les anomalies de fonctionnement sous garantie entrent dans la *backlog* d'anomalies.

Les prestations de maintenance corrective et préventive font l'objet de niveaux de service basés sur les exigences DICT¹ du produit numérique concerné.

¹ DICT : Disponibilité Intégrité Confidentialité Traçabilité – les exigences sont classées de 1 (exigences moindres) à 4 (exigences fortes).

Le DICT va de 1111 à 4444 et donne le niveau d'exigence attendu pour les 4 thématiques suivantes : Disponibilité Intégrité Confidentialité Traçabilité.

La **disponibilité** est l'aptitude d'une fonction à rendre le service attendu, pour une personne ou pour un système, en temps voulu et dans les conditions d'usage prévues. On étend cette définition, dans le présent document, à la notion de perte de donnée admissible pour un SI.

L'**intégrité** est la propriété permettant de s'assurer que les informations ne subissent aucune altération ou destruction, volontaire ou accidentelle, et conservent un format permettant leur utilisation lors de leur traitement, de leur conservation ou de leur transmission.

La **confidentialité** est la propriété permettant de s'assurer que seuls les utilisateurs ayant à en connaître et habilités dans les conditions normales prévues ont accès aux informations du SI lors de leur traitement, de leur conservation ou de leur transmission.

La **traçabilité** est la propriété qui garantit la conservation des enchaînements d'opérations fonctionnelles et / ou techniques sur le SI (ex. : la création d'un document, la validation d'un dossier, une prise de décision, etc.).

Les exigences attendues sont classées de 1 (exigences moindres) à 4 (exigences fortes).

Voir le détail dans le tableau ci-après.

Niveau de service Exigence	1	2	3	4
DISPONIBILITE	Garanties faibles Indisponibilité > 48h acceptable Perte de données > 24h d'activité acceptable	Garanties standards Indisponibilité de 4h à 48h acceptable Perte de données entre 2h et 24h d'activité acceptable	Garanties élevées Indisponibilité de 2h à 4h acceptable Perte de données < 2h d'activité acceptable	Garanties critiques Indisponibilité < 2h acceptable Perte de données non acceptable
INTEGRITE	Altération des données non vérifiée	Altération des données à détecter	Altération des données à détecter et corriger	Altération des données non acceptable
CONFIDENTIALITE	Données publiques, à diffuser	Données réservées à une diffusion interne (administration, partenaires identifiés)	Données sensibles, à diffusion restreinte (nominative), données à caractère personnel	Données confidentielles, à diffusion très restreinte ; données à caractère personnel sensible
TRACABILITE	Traçabilité non requise	Traçabilité des connexions nominative et horodatée	Traçabilité des actions (pour les fonctions sensibles) nominative et horodatée	Traçabilité des actions (pour les fonctions sensibles) nominative, horodatée et non répudiable

06. PROFIL DES INTERVENANTS

Les compétences attendues pour l'exécution de ce marché sont listées en annexe 1.