



**MINISTÈRE
DE L'ACTION
ET DES COMPTES
PUBLICS**

*Liberté
Égalité
Fraternité*

**Agence pour l'informatique
financière de l'État**

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES - CCTP

AMOA UX/UI et AMOE UI / développement front-end

**RÉFÉRENCE MARCHÉ AIFE :
26_AIFE_UX_UI_DEV_FRONT**

Numéro de consultation : 26_AIFE_UX_UI_DEV_FRONT

Le présent accord-cadre est porté par le ministère de l'Économie, des Finances et de la Souveraineté industrielle et Numérique

Direction ou service : **AGENCE POUR L'INFORMATIQUE FINANCIERE DE L'ETAT**

Adresse : **10, rue du Centre**

Code Postal : **93160**

Ville : **NOISY-LE-GRAND**

Siret : **11000201100044**

Téléphone : **01 57 99 95 62**

Il est représenté par Monsieur Emmanuel SPINAT, Directeur de l'AIFE ou par délégation par Madame Armelle DEFONTAINE, Secrétaire Générale de l'AIFE, et Monsieur Victor ENGELHARDT, Secrétaire Général adjoint de l'AIFE.

Adresse du profil d'acheteur : <http://www.marches-publics.gouv.fr>

GLOSSAIRE

Abréviation	Signification
AIFE	Agence pour l'Informatique Financière de l'État
AMOA	Assistance à Maîtrise d'Ouvrage
AMOE	Assistance à Maîtrise d'Œuvre
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BPU	Bordereau de Prix Unitaires
CCAP	Cahier des Clauses Administratives Particulières
CCTP	Cahier des Clauses Techniques Particulières
CI/CD	Continuous Integration / Continuous Deployment (intégration et déploiement continus)
Design OPS	Pratiques d'automatisation et d'industrialisation des flux entre design et développement
DINUM	Direction Interministérielle du Numérique
HF	Haute Fidélité (maquette graphique détaillée)
j.o.	Jours ouvrés
MOA	Maîtrise d'Ouvrage
MOE	Maîtrise d'Œuvre
POC	Proof Of Concept (preuve de concept)
PSSIE	Politique de Sécurité des Systèmes d'Information de l'État
PV	Procès-Verbal
RCN	Référentiel de Conception Numérique (design system de l'AIFE)
RGAA	Référentiel Général d'Amélioration de l'Accessibilité
RGPD	Règlement Général sur la Protection des Données
SemVer	Versionnement sémantique (Semantic Versioning)
SI	Système d'Information
SPA	Single Page Application
UI	User Interface (interface utilisateur)
UO	Unité d'Œuvre — prestation définie par un périmètre fonctionnel et un niveau de complexité
US	User Story
UX	User Experience (expérience utilisateur)
WCAG	Web Content Accessibility Guidelines (référentiel international d'accessibilité)

SOMMAIRE

1	OBJET DU MARCHÉ	5
2	CONTEXTE	6
2.1	Présentation de l'AIFE	6
2.2	Présentation des produits	7
2.3	Présentation du département	8
3	GOVERNANCE ET MODALITÉS D'EXÉCUTION COMMUNES	12
3.1	Interlocuteurs et organisation	12
3.2	Cadre agile et rituels de suivi	12
3.3	Comités de suivi	12
3.4	Rapport mensuel d'activité	14
3.5	Processus de création et d'évolution d'un composant RCN	14
4	EXIGENCES TRANSVERSALES	16
4.1	Exigences documentaires	16
4.2	Exigences d'accessibilité numérique (RGAA)	16
4.3	Exigences de sécurité	16
4.4	Exigences en matière de ressources humaines	35
4.5	Exigences de qualité logicielle et de niveaux de service (Lot 2)	36
4.6	Exigences méthodologiques et d'industrialisation	36
4.7	Exigences de traçabilité et de gouvernance	36
4.8	Exigences relatives à la relation avec des tiers	36
4.9	Exigences de transférabilité et de réversibilité	37
4.10	Exigences d'amélioration continue	37
5	LOT 1 — ASSISTANCE À MAÎTRISE D'OUVRAGE EN UX/UI	38
5.1	Objet et périmètre du Lot 1	38
5.2	Modalités d'exécution du Lot 1	38
5.3	Unités d'œuvre du Lot 1	39
5.3.1	L1-UX-P1 — Cadrage & Discovery	39
5.3.2	L1-UX-P2 — Conception & Prototypage	40
5.3.3	L1-UX-P3 — Tests utilisateurs	41
5.3.4	L1-UX-P4 — Validation & Recette UX/UI	42
5.3.5	L1-UX-P5 — Suivi & Amélioration continue	43
6	LOT 2 — ASSISTANCE À MAÎTRISE D'ŒUVRE UI / DÉVELOPPEMENT FRONT-END (RCN) 44	
6.1	Objet et périmètre du Lot 2	44
6.2	Modalités d'exécution du Lot 2	44
6.3	Unités d'œuvre du Lot 2	45
6.3.1	L2-DEV-P1 — Création/évolution de composant(s) UI RCN	45
6.3.2	L2-DEV-P2 — Implémentation d'interfaces et d'écrans	46
6.3.3	L2-DEV-P3 — Expertise architecture & gouvernance front-end	47
6.3.4	L2-DEV-P4 — Analytics & Plan de marquage	49
6.3.5	L2-DEV-P5 — Expertise & accompagnement en maintenance front-end	50

1 OBJET DU MARCHÉ

Le présent cahier des clauses techniques particulières (CCTP) définit les prestations attendues dans le cadre de l'accord-cadre multi-attributaires passé par l'Agence pour l'Informatique Financière de l'État (AIFE) portant sur des services de conception numérique et de développement front-end. Le marché est structuré en deux lots distincts :

- Lot 1 — Assistance à maîtrise d'ouvrage en UX/UI ;
- Lot 2 — Assistance à maîtrise d'œuvre UI / développement front-end (RCN).

Le présent accord-cadre répond aux enjeux stratégiques suivants pour l'AIFE :

- **Qualité et cohérence des interfaces :** garantir que l'ensemble des produits numériques de l'AIFE respecte les standards du RCN et offre une expérience utilisateur homogène et accessible à tous les types d'utilisateurs.
- **Alimentation et évolution du RCN :** faire du RCN un référentiel vivant, alimenté par les projets terrain (Lot 1) et mis en œuvre côté développement (Lot 2), afin de réduire les coûts et délais de production des interfaces numériques.
- **Accessibilité numérique :** s'assurer que les interfaces sont conçues et développées en conformité avec le RGAA, conformément aux obligations légales applicables aux services publics numériques.
- **Mesure des usages et analytics :** intégrer dès la phase de conception les besoins de mesure afin de disposer d'une connaissance fine des usages et d'orienter les arbitrages produit de l'AIFE.
- **Agilité et réactivité :** disposer d'une ressource prestataire flexible et mobilisable rapidement sur les bons de commande, capable de s'intégrer dans les équipes agiles de l'AIFE dans le respect des méthodes et outils en place.

2 CONTEXTE

2.1 Présentation de l'AIFE

Rattachée au ministre de l'Action et des Comptes publics, l'Agence pour l'Informatique financière de l'État (AIFE) est chargée du pilotage des systèmes d'information financière de l'État.

L'AIFE est un service à compétence nationale créé par le décret n°2005-122 du 11 février 2005 modifié par les décrets n° 2014-462 du 7 mai 2014 et n°2019-1543 du 30 décembre 2017. Sa gouvernance est interministérielle.

Les missions majeures de l'AIFE sont :

- Piloter l'urbanisation du Système d'Information Financière de l'État ;
- Maintenir en condition opérationnelle le système d'information Chorus de gestion financière de l'État et le système Chorus Pro de dépôt des factures électroniques de la sphère publique ;
- Maintenir en condition opérationnelle la plateforme des achats de l'État « PLACE » ;
- Piloter de nouveaux projets interministériels ou ministériels et leur intégration dans le système d'information Chorus ;
- Accompagner le changement dans les ministères et auprès des utilisateurs.

L'Agence exerce ces missions pour le compte de l'État, d'établissements publics ou d'autres personnes publiques.

L'AIFE est certifiée ISO 9001 depuis 2008 (dernier renouvellement en 2023), elle se compose d'un secrétariat général, d'une direction de programme, et de quatre délégations :

- Délégation Socle Numérique (DSN),
- Délégation aux Services Numériques Financiers (DSNF)
- Délégation Pilotage et Relation Usagers (DPRU)
- Délégation Innovation (DINNOV)

2.2 Présentation des produits

Les plateformes ci-après constituent l'environnement applicatif dans lequel peuvent s'inscrire les prestations du présent marché. Le titulaire est susceptible d'intervenir sur tout ou partie de ces produits, sans en assurer nécessairement la maîtrise d'ouvrage ni la responsabilité opérationnelle. Il est tenu d'en comprendre les enjeux fonctionnels et les contraintes techniques afin de garantir la cohérence et la qualité des livrables produits dans le cadre de chaque lot.

À ce titre, le titulaire devra s'assurer, tout au long de l'exécution du marché, de la bonne articulation de ses interventions avec les marchés existants portant sur ces produits. Il lui appartient d'identifier les périmètres d'intervention des autres titulaires, de coordonner ses actions avec eux et de signaler sans délai à l'AIFE toute situation susceptible de générer un chevauchement ou un conflit de périmètre.

À la date de notification du marché, les produits faisant l'objet d'un suivi actif sont les suivants :

- Chorus DT
- Chorus Pro
- Facturation Électronique
- Astra
- RCN

Le titulaire pourra également être amené à intervenir, ponctuellement ou en soutien, sur les produits suivants :

- PLACE
- Avis de publicité
- Consultation
- DUME
- PISTE
- eSignature
- Portail de support
- Portail de services
- Diapason
- Portail de documentation
- Aifervescence
- Site Agence
- Dépenses éclairées
- Chorus

2.3 Présentation du département

Le département Expérience Utilisateur et Qualité Numérique (UXQN), rattaché à la Délégation Innovation (DINNOV) de l'AIFE, assure la conception et la cohérence des interfaces des services numériques de l'agence. Il pilote le design system de l'AIFE — socle commun de composants réutilisables et de règles de conception — dont l'implémentation, principalement en environnement Angular, accompagne le développement des applications métiers.

À partir de 2026, ce dispositif s'inscrit dans une logique d'industrialisation progressive, visant à élargir son adoption et à automatiser son intégration dans les cycles de conception projet.

Le département UXQN accompagne les équipes projet dans la conception de leurs services, de la modélisation des parcours utilisateurs jusqu'à la recette des interfaces, en veillant à la qualité, à l'écoconception et à la conformité accessibilité. Il s'appuie sur des outils d'analytics pour orienter les évolutions produits dans une démarche d'amélioration continue, et sur la solution ASTRA pour centraliser le pilotage des informations réglementaires du parc applicatif.

En matière d'accessibilité numérique, le département UXQN conduit un programme pluriannuel de mise en conformité qui a permis d'atteindre un niveau global de conformité proche de 80 % sur les principaux parcours des services de l'AIFE. Ces travaux s'inscrivent dans les engagements de l'État en matière d'inclusion numérique et se poursuivent dans le cadre du maintien en condition opérationnelle des applications.

2.3.1 ASTRA

Astra est une application web développée par le département UXQN de l'AIFE. Elle permet aux équipes de créer, gérer et publier des déclarations d'accessibilité conformes au RGAA 4.1.2 (Référentiel Général d'Amélioration de l'Accessibilité), la norme française encadrant l'accessibilité des services numériques publics.

L'outil couvre l'intégralité du cycle de vie d'un audit d'accessibilité : saisie du contexte, enregistrement des résultats, gestion des dérogations, publication et archivage de la déclaration.

URL du service : <https://astra.aife.economie.gouv.fr/>

Fonctionnalités principales

Gestion des déclarations d'accessibilité

- Création et édition de déclarations d'accessibilité pour une application donnée
- Formulaire multi-étapes guidé : contexte d'audit → résultats → dérogations → récapitulatif

- Publication, archivage et historique de versions des déclarations

Contexte d'audit

- Sélection du référentiel (RGAA 4.1.2)
- Configuration des pages auditées, des environnements de test, des outils et technologies utilisés

Résultats d'audit

- Saisie des non-conformités identifiées
- Dépôt de fichiers de résultats
- Synthèse automatique du taux de conformité

Dérogations et exemptions

- Qualification et documentation des dérogations
- Gestion des contenus exemptés selon les règles RGAA

Gestion des accès

- Gestion des utilisateurs et de leurs rôles
- Authentification sécurisée (JWT + bcrypt)
- Réinitialisation de mot de passe

Conformité légale

- Gestion des CGU (Conditions Générales d'Utilisation)
- Mentions légales et politique de confidentialité (conformité CNIL)
- Gestion du consentement aux cookies

Stack technique

Couche	Technologie
Frontend	Angular 19, TypeScript 5.5, SCSS
UI Components	@rcn/ngx-rcn 2.3.1 (bibliothèque interne RCN)
Backend	Node.js 22, Express.js 4.18
Base de données	PostgreSQL 16
Authentification	JWT, bcrypt
Rendu	Angular SSR (Server-Side Rendering) avec Express
Infrastructure	Docker + Docker Compose, Nginx (serveur statique)
Données RGAA	Fichiers JSON embarqués (critères RGAA 4.1.2, contenus exemptés)

2.3.2 Librairie Figma

La Bibliothèque RCN - Composants est la bibliothèque Figma officielle du département UXQN de l'AIFE. Elle constitue la source de vérité design pour l'ensemble des composants d'interface utilisateur du Référentiel de Conception Numérique (RCN), le design system des services numériques AIFE.

Elle est le pendant Figma de la librairie Angular ngx-rcn : tout composant présent dans la bibliothèque Figma a (ou devrait avoir) son équivalent dans le code Angular. Elle sert à la fois aux designers pour composer des maquettes et aux développeurs front-end pour cadrer l'implémentation.

Design tokens

La bibliothèque embarque deux collections de variables Figma qui servent de référence pour tous les composants.

- **RCN-Colors** — Variables de couleur Tokens sémantiques couvrant les couleurs de composants (ex. rcn-component/footer/navigationLink, rcn-component/footer/navigationLinksBackground) et les couleurs fondamentales (ex. rcn-core-color/deco/Color). Ces variables alimentent directement les fichiers CSS/SCSS de ngx-rcn.
- **RCN Sizes** — Variables de dimensionnement et d'espacement pour exemple :
 - Sizing : rcn-core-sizing/050 à rcn-core-sizing/1000 — tailles standardisées (width/height)
 - Spacing : rcn-core-spacing/0 à rcn-core-spacing/500 — espacements entre éléments (gap)

2.3.3 Librairie Angular

La librairie Angular, ngx-rcn, officielle du département UXQN de l'AIFE. Elle fournit un ensemble de composants, directives et services réutilisables qui implémentent le Référentiel de Conception Numérique (RCN), le design system utilisé pour les services numériques de l'État.

L'objectif est double : garantir la cohérence visuelle des interfaces entre les différentes applications du périmètre, et assurer leur accessibilité en conformité avec les standards RGAA et DSFR.

La librairie est publiée sous le nom de package @rcn/ngx-rcn sur le registre NPM interne GitLab.

Fonctionnalités principales

La librairie expose plus de 40 composants UI couvrant l'ensemble des besoins d'une application

Navigation & mise en page - Composants structurels : Header, Footer, Navigation principale, Navigation secondaire, Fil d'Ariane, Liens d'évitement, Pagination, Barre d'outils.

Formulaires - Champ de saisie : Select, Checkbox, Radio, Toggle, Combobox, Double input, Slider, Checkbox enrichi, Radio enrichi, Import de fichier, Date multi-champ, Fieldset.

Contenus & feedback : Bouton, Groupe de boutons, Lien, Badge, Tag, Alerte, Mise en avant (Callout), Carte, Média, Pictogramme, Résumé.

Composants avancés : Modal, Accordéon, Liste détaillée, État vide, Stepper, Onglets, Tableau, Treegrid, Contrôle segmenté, Bouton flottant, Menu d'action, Barre de recherche, Gestionnaire de consentement, Filtre, Tri, Transcription, Identification.

La librairie supporte 4 thèmes visuels : **Chorus**, **Chorus Pro**, **Piste** et **DSFR**, cela correspond aux familles applicatives de l'AIFE.

Stack Technique

Framework	Angular 19 (compatible Angular 14+)
Langage	TypeScript 5.6
Build	ng-packagr 19
Documentation interactive	Storybook 8 (222 stories)
Documentation API	Compodoc
Qualité	ESLint 9 + Prettier 3
Tests	Karma + Jasmine
Versioning	Semantic Versioning (Conventional Commits)

3 GOUVERNANCE ET MODALITÉS D'EXÉCUTION COMMUNES

3.1 Interlocuteurs et organisation

Le titulaire désigne un chef de projet ou responsable de compte unique, interlocuteur de l'AIFE pour toute la durée de l'accord-cadre. Tout changement de référent doit être notifié à l'AIFE avec un préavis minimum de quinze (15) jours ouvrés.

3.2 Cadre agile et rituels de suivi

Les prestations s'inscrivent dans un cadre de travail agile. L'unité de temps de référence est le sprint de deux (2) semaines. Le titulaire adopte les rituels agiles de l'AIFE et y participe activement selon le périmètre défini au bon de commande :

- Sprint Planning (début de sprint) : définition et priorisation du backlog du sprint, estimation des UO et engagement du titulaire ;
- Daily stand-up (quotidien, ~15 min) : point d'avancement, blocages, synchronisation avec l'équipe AIFE ;
- Sprint Review (fin de sprint) : démonstration des livrables réalisés à la MOA et aux parties prenantes, recueil des retours ;
- Rétrospective (fin de sprint) : amélioration continue des pratiques de l'équipe.

3.3 Comités de suivi

Les comptes rendus de réunions formelles (comités de pilotage, lancement, clôture) sont rédigés par le titulaire dans un délai de trois (3) jours ouvrés et soumis à validation de l'AIFE. Les cérémonies agiles (Sprint Planning, Review, Rétrospective) font l'objet d'une note de synthèse partagée dans l'outil de gestion de projet de l'AIFE.

Pour le présent marché, les instances de pilotage et comités prévus sont les suivants.

3.3.1 Comité contractuel

Le Comité contractuel se réunit tous les trois mois. Cette périodicité peut être revue d'un commun accord entre le titulaire et l'AIFE

Le titulaire organise le 1er comité de pilotage au plus tard (3) mois après la réunion de lancement du marché public, dans le respect des dates proposées par l'AIFE.

Le support de réunion et le compte-rendu du comité de pilotage sont rédigés par le titulaire. Le titulaire les adresse par courrier électronique aux membres du comité pour validation.

Le comité contractuel a pour objet :

- De réaliser un bilan des prestations ;
- De présenter l'évaluation de la qualité des prestations par l'AIFE ;
- De réaliser une présentation des indicateurs ;

- D'assurer le suivi contractuel du marché public (émission des bons de commande, des PV d'admission, etc.) ;
- D'examiner l'adéquation des moyens aux besoins : moyens humains et logistiques affectés au marché public et de manière générale pour assurer le suivi RH ;
- De résoudre les litiges et les divergences d'interprétation du marché public.

3.3.2 Comité de pilotage

Le Comité de pilotage se réunit tous les trois (3) mois. Cette périodicité peut être revue d'un commun accord entre le titulaire et l'AIFE

Le comité de pilotage comprend à minima le Directeur de projet du titulaire.

Le titulaire prépare un rapport d'avancement des prestations qu'il adresse à l'AIFE au plus tard 5 (5) jours ouvrés avant la tenue de chaque comité de pilotage.

Le titulaire organise le 1er comité de pilotage au plus tard trois (3) mois après la réunion de lancement du marché public, dans le respect des dates proposées par l'AIFE.

Le titulaire intègre à l'ordre du jour du premier comité de pilotage une proposition de modalités pratiques de fonctionnement du comité de pilotage, et prend en compte préalablement au comité de pilotage les précisions de l'AIFE sur ce point.

Le compte-rendu du comité de pilotage est rédigé par le titulaire. Le titulaire l'adresse par courrier électronique aux membres du comité pour validation.

Le comité de pilotage a pour objet :

- De vérifier l'avancement des prestations au regard des indicateurs définis au préalable et d'assurer le pilotage du marché public ;
- De s'assurer du respect du calendrier global du projet et des niveaux d'engagement de résultat ;
- De gérer les risques liés au pilotage du marché public ;
- D'examiner l'adéquation des moyens aux besoins : moyens humains et logistiques affectés au marché public et de manière générale assurer le suivi RH.
- De discuter et apporter une solution de premier niveau aux points bloquants
- De suivre les incidents de sécurité, notamment, les plans d'action de remédiation des incidents de sécurité
- De vérifier la bonne application du processus des entrées/sorties du personnel du titulaire

3.3.3 Réunion de lancement technique du marché

En plus d'une réunion de démarrage administratif du marché, évoquée au CCAP, une réunion de lancement technique du marché est prévue.

Le titulaire organise une réunion de lancement au plus tard deux (2) semaine après le démarrage administratif du marché.

Cette réunion a pour objet de cadrer les conditions d'exécution du marché : présentation des équipes, cadrage technique, prise en main de l'environnement RCN et définition du calendrier prévisionnel des premières prestations. Un compte-rendu est rédigé par le titulaire et adressé à l'AIFE pour validation dans un délai de cinq (5) jours ouvrés.

3.3.4 Réunion de lancement et clôture des bons de commande

Lors de l'émission et de la clôture d'un bon de commande ont lieu les réunions suivantes :

- Réunion de lancement pour chaque bon de commande : objectifs, périmètre, UO et niveau de complexité retenus, constitution de l'équipe ;
- Réunion de clôture de bon de commande : bilan, archivage des livrables, retours d'expérience.

3.4 Rapport mensuel d'activité

Le titulaire fournit chaque mois un rapport reprenant : récapitulatif des bons de commande actifs, avancement des UO en cours, alertes, indicateurs de performance et prévisions. Ce rapport est transmis au plus tard le 5 du mois suivant la période de référence.

3.5 Processus de création et d'évolution d'un composant RCN

La création ou l'évolution d'un composant au sein du Référentiel de Conception Numérique (RCN, dénomination susceptible d'évoluer au cours de l'exécution du marché) suit un processus formalisé, impliquant les deux lots et deux jalons de validation interne. Ce processus garantit la cohérence et la qualité du RCN, en s'assurant que chaque nouveau composant est validé avant développement et avant mise en production.

N°	Étape	Responsable	Livrables et condition de passage
1	Identification du besoin composant	Lot 1 + MOA AIFE	Fiche de besoin composant : contexte d'apparition dans les projets, cas d'usage cibles, écart constaté avec la librairie RCN existante, transmise à l'AIFE.
2	Ébauche et du cadrage composant	Lot 1	Esquisse low-fi du composant et note de cadrage : périmètre fonctionnel, variantes identifiées, contraintes d'accessibilité et d'alignement RCN.

N°	Étape	Responsable	Livrables et condition de passage
3	Validation interne de lancement	AIFE	Décision go / no-go formalisée par l'AIFE. Condition obligatoire avant engagement de l'étape 4. En cas de no-go, la fiche de besoin est retournée au Lot 1 pour révision.
4	Conception haute fidélité Figma	Lot 1	Composant Figma haute fidélité : tokens de design, variantes, états (chargement, erreur, vide, succès), responsive, accessibilité. Spécifications de handoff : comportements, cas limites, règles d'accessibilité RGAA.
5	Développement Angular du composant	Lot 2	Composant Angular livré avec : tests unitaires et tests d'accessibilité automatisés (axe-core ou équivalent), documentation Storybook (stories, props, variantes, états, notice d'accessibilité), rapport de couverture de tests.
6	Validation interne finale	AIFE	Décision go / no-go formalisée par l'AIFE. Condition obligatoire avant mise en production. En cas de no-go, les corrections sont prises en charge par le lot responsable de l'anomalie constatée.
7	Mise en production (MEP)	AIFE + Lot 2	Publication du composant dans la librairie RCN (Figma et Angular). Mise à jour du changelog (SemVer). Notification aux équipes produit de l'AIFE.

Les jalons de validation interne (étapes 3 et 6) sont sous la responsabilité exclusive de l'AIFE. Le titulaire du Lot 1 ne peut engager la phase de conception haute fidélité (étape 4) sans validation formalisée de l'AIFE à l'étape 3.

Le déclenchement de ce processus est formalisé dans les bons de commande concernés. Lorsqu'une mission relevant du Lot 1 fait apparaître un besoin en nouveau composant RCN, le titulaire le documente dans une fiche de besoin transmise à l'AIFE dans un délai de cinq (5) jours ouvrés suivant l'identification du besoin.

4 EXIGENCES TRANSVERSALES

Les exigences décrites dans la présente section s'appliquent à l'ensemble du marché et constituent le socle commun aux deux lots. Elles s'ajoutent et complètent les prestations décrites en partie 6 (Lot 1) et partie 7 (Lot 2). En cas de contradiction avec une clause spécifique à un lot, la clause la plus contraignante prévaut.

4.1 Exigences documentaires

Tous les livrables documentaires sont rédigés en langue française, sous format modifiable (.docx, .xlsx, .md, .fig selon la nature). La police et la mise en page respectent la charte documentaire de l'AIFE transmise en début de marché. Chaque livrable comporte à minima :

- Un historique des versions (auteur, date, objet de la modification) ;
- Un cartouche d'identification (référence marché, bon de commande, lot, titulaire) ;
- Une validation traçable (circuit de relecture et d'approbation MOA).

Le titulaire alimente le référentiel documentaire de l'AIFE et assure l'archivage des versions validées à la clôture de chaque bon de commande.

4.2 Exigences d'accessibilité numérique (RGAA)

L'accessibilité est intégrée dès la conception (Lot 1) et vérifiée à chaque livraison (Lot 2). Le titulaire :

- applique les critères du RGAA dans sa version en vigueur à l'ensemble des écrans, composants et parcours livrés ;
- Outille les vérifications automatisées (axe-core ou équivalent) dans les pipelines CI/CD (Lot 2) ;
- Réalise, sur périmètre défini au bon de commande, des audits RGAA manuels et produit les déclarations d'accessibilité associées ;
- Intègre dans la recette un taux de conformité RGAA cible, sauf dérogation explicitement motivée au bon de commande.

Tout écart de conformité fait l'objet d'un plan de remédiation documenté et priorisé.

4.3 Exigences de sécurité

4.3.1 Exigences liées aux postes d'administration et à leur raccordement

4.3.1.1 Principes généraux

Quel que soit les solutions retenues, le titulaire se doit de respecter les recommandations de l'ANSSI et notamment, mais pas seulement, celles traitant de l'administration sécurisée des systèmes d'information, le nomadisme numérique et l'interconnexion d'un système d'information à Internet (https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-admin_securisee_si_v3-0.pdf). Les éléments fournis dans ce chapitre ont pour but de

compléter ou préciser certaines des bonnes pratiques à tenir, mais ne viennent en aucun cas contredire ou altérer les recommandations de l'ANSSI.

4.3.1.2 *Ressources mises en jeu*

Pour mener à bien ses missions, le titulaire a besoin d'accéder à l'ensemble des environnements non productifs du SI et notamment aux différents outils permettant la gestion et l'administration du système d'information. On ne parle pas ici des accès aux services et applications exposés aux utilisateurs finaux, mais bien des outils ayant une incidence directe sur le fonctionnement même du SI.

Pour ce faire, le titulaire met à disposition tous les moyens nécessaires à son activité, en conformité avec les principes généraux sus-indiqués. Sans être exclusif, il doit mettre en place et disposer :

- De sites sécurisés permettant l'hébergement des équipes,
- De postes de travail incluant le système, les licences et outils nécessaires à la prestation,
- De moyens d'authentification compatibles avec les solutions mises en place au sein du SI,
- De moyens d'accès sécurisés (l'AIFE pouvant proposer des solutions), en particulier si besoin de nomadisme (télétravail et/ou astreintes par exemple) et de transferts de données sécurisées.

Une validation par les équipes techniques et SSI de l'administration est réalisée avant la mise en place de l'ensemble de ces composantes, l'ensemble étant documenté au travers d'un livrable amenant explications et preuves de l'implémentation.

4.3.1.3 *Les sites*

Les équipes de développement, de maintenance et d'exploitation sont hébergées au sein de locaux mis à disposition par le titulaire en respectant les exigences de sécurité associées Cf.§ Exigences en termes de localisation et d'usage de la langue française). Elles peuvent également bénéficier d'un accès nomade dès lors que les conditions sont réunies pour cela (voir chapitre suivant et guides ANSSI), que ce soit en solution nominale (télétravail/astreinte) ou en mode secours si incident au sein des locaux du titulaire.

4.3.1.4 *Le poste d'administration*

Il faut bien distinguer les différents types de postes de travail, les allouer en fonction du rôle de chacun et surtout de la sensibilité des accès qui y sont effectués.

Un poste bureautique ne peut être utilisé pour l'administration d'un SI, même s'il est issu d'une entreprise et même s'il est utilisé au travers d'une solution de rebond, bastion ou VDI. Il sera réservé à un usage de type utilisateur final dit « front office » et restera naturellement nécessaire aux échanges par mail.

Il en va de même pour un poste servant aux développements qui par construction nécessite de forts échanges avec diverses ressources situées sur Internet. Par défaut, ce dernier ne pourra interagir avec le SI qu'au travers d'une zone de dépôts et en aucun cas servir à une connexion « back office » sur le SI (quel que soit l'environnement). A contrario, le poste d'administration est quant à lui totalement dédié à l'administration des SI et donc à l'accès « back office » (Il peut par contre être mutualisé entre plusieurs SI de même sensibilité). Cet emploi implique le respect d'exigences tant en termes d'outillage que d'usage. Sans être exhaustif, le poste d'administration doit à minima respecter les principes suivants :

- Chiffrement du disque,
- Firewall actif,
- Antivirus actif et se maintenant à jour,
- Aucun usage de messagerie,
- Aucune connexion Internet (usage d'une liste blanche limitée au seul maintien en condition opérationnelle du poste et à la connexion au SI administré),
- Désactivation du stockage sur port USB (usage exclusif pour les médias d'authentification),
- Aucun droit d'administration,
- Authentification forte sur le système avec compte dédié (annuaire dédié),
- Usage d'un coffre-fort pour le stockage des comptes/mots de passe,
- Usage des postes depuis un lieu sûr (hors lieu public),
- Limitation d'outils aux seuls besoins d'administration. Cas particulier :
 - Un développeur ayant des besoins d'accès de type « back office » devra soit accepter les exigences du poste d'administration soit faire usage, en plus de son poste de développement, d'un poste d'administration.

4.3.1.5 Les accès

Les accès au SI sont réalisés au moyen de solutions réseaux sécurisées, que ce soit au travers d'une liaison dédiée, d'un VPN IPSEC (raccordement site à site) ou d'un VPN SSL (raccordement nomade notamment). Dans ce dernier cas, des contrôles de conformité du poste seront obligatoires (éléments prouvant l'origine du poste, mises à jour du poste d'administration, connexion exclusive au VPN, etc.) ainsi qu'une authentification à minima par multi facteur.

L'ensemble des flux y transitant seront chiffrés (TLS1.3) et filtrés via firewall réseau et/ou système.

Par ailleurs, et sauf exception, l'accès n'est pas réalisé directement sur les ressources à administrer mais se fait au travers de rebonds/bastions permettant l'authentification de l'utilisateur du poste d'administration, la gestion des habilitations et la journalisation des actions réalisées. Une solution basée sur VDI est également possible, mais ne remettra pas en cause, ni les obligations liées aux postes d'administration, ni l'usage de bastions/rebonds mis en place.

Si l'utilisateur, depuis son poste d'administration, a besoin d'accéder à des ressources se trouvant sur Internet (GED, outils servant à la maintenance, sites éditeurs, etc.) deux options se proposent à lui :

Accès indirect au travers de serveurs de rebonds bureautiques (avec interdiction du transfert de données) à mettre en place par le titulaire au besoin dans le cadre de sa prestation,

Accès direct au travers d'une solution de proxy présent au sein du SI et ouvert suivant une validation de l'AIFE (gestion centralisée).

Un cas particulier concerne les outils de collaboration permettant aux équipes d'interagir entre-elles mais surtout de permettre des interventions liées au support éditeur. Ceux-ci sont autorisés au cas par cas (à date l'usage de la Webconférence de l'Etat et de MS Teams sont tolérés).

4.3.2 Exigences sécurité - Système de management de la sécurité

4.3.2.1 Introduction

La prise en compte de la sécurité par les Titulaires s'appuie sur un système de management de la sécurité (SMSI) en conformité avec l'ISO 27001, et sur une analyse de risques (méthode EBIOS) ainsi que sur la gestion des risques en conformité avec l'ISO 27005 et le RGS (Référentiel Général de Sécurité).

Les titulaires se doivent de prendre en compte l'IGI 1300/SGDN/PSE/PSD du 15 novembre 2020 relative à la protection du secret de la défense nationale dans toutes ses composantes.

Les titulaires se doivent de prendre en compte le Règlement Général sur la Protection des Données dans toutes ses composantes.

4.3.2.2 État de l'art

Conformément à l'article 7.2 « Devoir d'information, de conseil et d'alerte » du CCAP, le titulaire conçoit, met en œuvre les systèmes d'informations sous sa responsabilité conformément à l'état de l'art en matière de sécurité des systèmes d'information. Il doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière. Toutefois, il doit respecter les exigences suivantes pour les services Web et de messagerie :

Interfaces web :

- les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, etc.) ou une technologie en particulier ;
- les mécanismes cryptographiques TLS (https) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications ;
- l'utilisation de la technologie HSTS est exigée ;

- les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;
- une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est appliquée pour se protéger contre les injections de contenus actifs malicieux (cf. standards de sécurité du ministère des finances) ;
- les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact identifiés. ·

Services de courriels :

- les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, etc.) ;
- la mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (SPF), signature numérique (DKIM), politique de sécurité liant le tout (DMARC))

Les référentiels que les titulaires doivent respecter sont consultables à l'URL <https://aife.economie.gouv.fr/referentiel/securite>

4.3.2.3 Politique, organisation et gouvernance de la sécurité

Politique de sécurité du titulaire : le titulaire applique et fait appliquer à ses sous-traitants la politique de sécurité du présent marché. Cette politique de sécurité traite notamment des thèmes suivants :

- Organisation de la Sécurité des SI ;
- Application de la Politique de Sécurité des SI ;
- Évaluation de la sensibilité et protection des documents ;
- Gestion des ressources humaines ;
- Sécurité physique des locaux et des salles informatiques ;
- Architecture et exploitation des SI : réseaux, systèmes ;
- Sécurité des postes de travail ;
- Sécurité des supports numériques ;
- Gestion des autorisations et contrôle d'accès logique aux ressources ;
- Développement et maintenance des systèmes ;
- Gestion des incidents et des alertes ;
- Gestion de la continuité d'activité des SI ;
- Conformité et démarche de contrôle interne ;
- Localisation des données.

Organisation de la sécurité adéquate : le titulaire définit une organisation de la sécurité afin de respecter l'ensemble des contraintes émises par l'acheteur.

- Existence d'un correspondant de sécurité : le titulaire désigne, dans les dix jours calendaires qui suivent la notification du lot, parmi son personnel un

correspondant sécurité pour toute la durée de la prestation. L'AIFE se réserve le droit de récuser ce correspondant sécurité, pour de justes motifs, dans un délai de dix jours calendaires à compter de sa désignation par le titulaire. Tout remplacement de ce correspondant doit être notifié à l'acheteur conformément à l'article 3.1.2 du CCAP. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.

Ce correspondant est notamment :

- L'interlocuteur privilégié de l'acheteur pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'acheteur ou le titulaire suite à des incidents de sécurité opérationnels ;
- Chargé du maintien et de la mise en application du PAS et des exigences du CCTP.
- La rédaction d'un dossier de sécurité sur le périmètre des prestations réalisées (voir paragraphe suivant) ;
- La rédaction d'un dossier de sécurité des SI (voir paragraphe suivant) ;
- Organiser les comités de suivi sécurité : convocation, proposition d'ordre du jour, rédaction des comptes rendus ;
- Présenter l'avancement des plans d'actions sécurité consécutifs aux audits et contrôles :
 - Sur le périmètre des prestations ;
 - Sur les SI en charge ;
- Suivre les plans d'actions issus des audits de sécurité effectués par le titulaire ou par l'administration ;
- Assister l'administration pour l'organisation des audits de sécurité ;
- Réaliser une analyse de risques au format EBIOS des activités du Titulaire ;
- Mettre à jour, suivre et présenter les risques de sécurité ;
- Suivre l'application des correctifs de sécurité ;
- Déclarer et suivre les incidents liés à la sécurité de l'information (dont les incidents ayant un impact sur les personnes) ainsi que les plans d'actions curatifs et préventifs associés ;
- Présenter les résultats des tests annuels du plan de reprise d'activité du titulaire ;
- Faire appliquer et contrôler le respect des engagements de confidentialité des employés partenaires et sous-traitants ; et plus généralement de faire prendre en compte les besoins de sécurité de l'administration par les partenaires et sous-traitants, suivant les objectifs décrits dans le PAS.
- Constituer et présenter les indicateurs sécurité tels que définis dans les CCTP des lots.
- Vérifier la bonne compréhension et la bonne application des règles et directives de sécurité ;
- Assurer la promotion de la sécurité (sensibilisation sécurité auprès du personnel des équipes du Titulaire) ;
- Réaliser l'ouverture des fiches d'incidents de sécurité potentiels ou avérés.

Mise en œuvre d'une gestion de risques et son suivi : le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses propres sous-traitants.

Gestion de crise sécurité : sur son domaine de responsabilité SI, le titulaire applique le processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'acheteur le respect des engagements de service et de sécurité SI contractualisés. Ce plan précise au minimum :

- les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;
- la composition de la cellule de crise : fonctions et responsabilités des membres (acheteur et titulaire). La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ;
- les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).

4.3.2.4 Pilotage de la sécurité

Un comité de suivi trimestriel a lieu avec l'AIFE, afin de gérer la mise en place et l'évolution du volet sécurité des prestations : respect du calendrier, conformité des prestations, respect de l'obligation de collaboration, validation des améliorations pour accroître la sécurité et mise à jour des plans d'assurance sécurité (PAS) et des analyses de risques. Il traite également des questions techniques touchant à la sécurité : collaboration dans la gestion des droits et la gestion des incidents, détection des anomalies et préconisation d'améliorations, exploitation des résultats des audits de contrôle des prestations sécurité, suivi des plans d'action issus d'audits, suivi du maintien en condition de sécurité, etc...

C'est également ce comité qui traite du respect des obligations liées à la loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés : mise à jour du registre de traitements, suivi des incidents impliquant la violation de données à caractère personnel, désignation d'un interlocuteur RGPD, ...

Les instances de pilotage de la sécurité des solutions réunissant l'AIFE et les Titulaires sont organisées selon les modalités décrites dans la prestation de pilotage suivantes.

4.3.2.5 Dossier de sécurité

Le Titulaire fournit dans le cadre des prestations d'initialisation un dossier de sécurité.

Ce dossier de sécurité comprend :

- Le Plan d'assurance sécurité (PAS) ;
- L'identification du correspondant sécurité ;
- L'identité et les coordonnées du Délégué à la Protection des Données du Titulaire ;

- La prise en compte des besoins de sécurité au regard du périmètre des prestations et des responsabilités du Titulaire ;
- Les non-conformités aux exigences de sécurité du marché ;
- Les supports de promotion de la sécurité à destination des équipes du Titulaire ;
- Le choix des solutions au regard de la couverture des exigences du présent marché et des PSSI ;
- L'analyse de risques (méthodologie EBIOS) ;
- L'identification des risques résiduels portant sur les SI et les données à caractère personnel ;
- Les mesures de couverture de ces risques résiduels proposées.

4.3.2.6 Plan d'Assurance Sécurité

Chaque titulaire est responsable de la rédaction initiale et de la mise à jour du Plan d'Assurance Sécurité (PAS), suivant le modèle consultable sur le site de l'ANSSI: (https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf)/ paragraphe dénommé « LE PLAN D'ASSURANCE SÉCURITÉ » recommandé par l'ANSSI ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité du donneur d'ordres pendant toute la durée des prestations.

Ce document décrit les dispositions que chaque titulaire s'engage à mettre en œuvre pour garantir le respect des exigences de sécurité dans le cadre des prestations. Il définit en particulier l'organisation qui est mise en place, la méthodologie à suivre pour gérer la sécurité du projet et les mesures techniques, organisationnelles et procédurales qui sont mises en œuvre.

Chaque titulaire s'engage à exécuter ses obligations en termes de sécurité des systèmes d'information décrits dans le Plan d'Assurance Sécurité.

4.3.2.7 Promotion de la sécurité

Le Titulaire fournit des supports de promotion de la sécurité présentant a minima :

- Les éléments fondateurs de la sécurité et de la protection des données à caractère personnel ;
- Les bonnes pratiques en matière de respect des exigences de sécurité du présent marché, de la PSSI de l'AIFE et des procédures de sécurité ;
- La traduction des bonnes pratiques dans le quotidien des acteurs concernés ;
- Le processus de gestion de crise de l'AIFE ;
- Les risques liés à la génération du code source par l'IA ;
- En complément, les développeurs peuvent également être formés sur les outils d'IA pour l'optimisation de leurs requêtes (prompt engineering) afin d'améliorer la qualité et la sécurité du code généré.

4.3.2.8 Exigences de sécurité envers les titulaires

L'ensemble des thèmes de l'ISO 27002 ainsi que les éléments des PSSI AIFE s'appliquent au Titulaire et en priorité les thèmes suivants :

- Organisation ;
- Classification des informations ;
- Ressources Humaines ;
- Sécurité Physique ;
- Exploitation éventuelle des infrastructures et applications dans les locaux du Titulaire et raccordées aux SI de la Commande publique ;
- Cloisonnement des environnements bureautiques et d'administration des systèmes ;
- Exploitation de la plate-forme de Développement ;
- Procédures d'exploitation à maintenir ou à faire évoluer dans le cadre des activités (modules) du marché ;
- Contrôle d'accès logique (Connexion aux divers environnements) ;
- Développement et maintenance ;
- Gestion des incidents de sécurité ;
- Gestion de la continuité d'activité ;
- Éléments de preuve de conformité ;
- Les exigences concernant la confidentialité (liée à l'authentification et la gestion des privilèges des utilisateurs du Titulaire ayant accès aux SI de la Commande publique) ;
- Les exigences inhérentes à l'externalisation (risques liés aux interventions à distance, infrastructure mutualisée).

4.3.2.9 Gestion des biens

Séparation des données de l'acheteur et des données d'autres clients : le titulaire conserve et traite les données de l'acheteur de manière séparée de ses propres données ou de données d'autres clients du titulaire. Le titulaire doit restreindre l'accès aux données de l'acheteur suivant le principe de restriction au besoin d'en connaître.

Protection de la documentation de l'acheteur sur support papier : le titulaire assure la protection de la documentation de l'acheteur sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.

Modalités d'échanges d'informations : le titulaire garantit que les modalités de stockage et d'échanges d'informations par mail permettent d'en assurer la confidentialité et l'intégrité. Notamment pour les échanges par messagerie, le titulaire utilise des adresses de messagerie en finances.gouv.fr (créées à l'initialisation).

Échange de supports : le titulaire garantit que les supports échangés ou à connecter sur un SI de l'acheteur n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir à l'acheteur.

Marquage des ressources techniques : le titulaire applique des règles de marquage sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles ou classifiées.

Supports de stockage hébergeant des données de l'acheteur : le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données de l'acheteur, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée. Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse de l'acheteur.

Maintien à jour et mise à disposition des données relatives à la prestation : le titulaire maintient à jour et est en mesure de mettre à disposition de l'acheteur toutes les données relatives à la prestation.

Le titulaire fournit systématiquement toute la documentation générée dans le cadre de la prestation à l'acheteur pour archive.

4.3.2.10 Sécurité physique

Changement de localisation géographique des services et des données : en cas de changement de localisation des données ou services, le titulaire en informe préalablement l'acheteur.

Localisations : A titre d'information, la PSSI de l'État prévoit que les informations de l'Administration considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont exploitées sur le territoire national.

Les données et les prestations doivent être hébergées de préférence sur le territoire national, à défaut dans l'Union Européenne. Le titulaire identifie tous les titulaires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation. Les localisations doivent être fournies dans la réponse des candidats.

Le candidat devra également s'assurer du cloisonnement des données de l'AIFE vis-à-vis de ses autres clients et de l'absence d'exposition (hébergement, services SaaS, etc.) à des lois extraterritoriales.

Contrôle d'accès physique aux bâtiments du titulaire : les bâtiments du titulaire hébergeant son personnel dans le cadre de la prestation doivent être équipés d'un dispositif de contrôle d'accès individuel. Les accès physiques aux bâtiments en question doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du titulaire. Le titulaire dispose d'une procédure de gestion des accès physiques aux bâtiments du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et de suppressions d'accès. Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les bâtiments du titulaire.

Contrôle des accès aux ressources techniques du titulaire : le titulaire garantit que les accès physiques aux salles informatiques sont strictement restreints aux besoins opérationnels des différentes populations présentes sur les sites utilisés dans le cadre de la prestation. Les accès sont équipés d'un dispositif de contrôle d'accès individuel. Le titulaire dispose d'une procédure de gestion des accès physiques aux locaux techniques du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès. Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources de l'acheteur et les équipements de sûreté.

Protection intrusion physique des locaux techniques du titulaire : les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, etc.) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements sont opérationnels 24h/24h et 7j/7j. Les moyens de protection sont adaptés aux moyens de détection et de réaction. En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

Accompagnement des visiteurs : le titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. Il dispose également d'une procédure pour l'accès des véhicules au site. En particulier, les personnes extérieures nécessitant un accès aux salles hébergeant des ressources informatiques (techniciens, visiteurs, maintenance, etc.) sont accompagnées par une personne habilitée.

Protection des plateaux mutualisés : en cas de mutualisation de ses plateaux, le titulaire met en place les mesures pour protéger les espaces attribués pour la prestation effectuée pour l'acheteur (accès au poste par badge, blocage session automatique après un certain temps d'inutilisation, câble de sécurité pour le matériel fourni par l'acheteur, etc.).

Étanchéité physique des ressources informatiques : les salles hébergeant les ressources informatiques utilisées dans le cadre de la prestation ne partagent pas le même bâtiment avec d'autres fonctions, particulièrement des bureaux n'appartenant pas à l'organisation. Si l'espace doit être mutualisé pour des raisons économiques, alors la salle hébergeant des ressources informatiques utilisées dans le cadre de la Prestation de l'acheteur n'a pas de murs adjacents à d'autres bureaux. Le titulaire met en place des moyens garantissant une étanchéité physique entre les infrastructures physiques dédiées à l'acheteur de celles des autres clients au sein des salles informatiques :

- La salle hébergeant des matériels de l'acheteur doit si possible lui être dédiée ;

- Dans le cas où la séparation physique des salles n'est pas possible, le titulaire fournit à l'acheteur une solution de « suite privative » au sein de la salle multi-clients, isolée physiquement du reste de la salle par un grillage descendant plus bas que le faux plancher et montant plus haut que le faux plafond.

4.3.2.11 Sécurité des réseaux et de l'exploitation

Cloisonnement des environnements informatiques : Le titulaire devra s'assurer que les environnements applicatifs utilisés dans le cadre de la prestation respectent les contraintes de cloisonnement (physique ou logique) définies par l'exploitant en charge de l'infrastructure et de l'exploitation.

Sécurisation des flux d'administration : le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration utilisés pour la prestation doivent être dédiés et n'avoir accès ni à Internet, ni à aux infrastructures bureautiques du titulaire.

Règles de sécurité et d'exploitation : Le titulaire s'engage à respecter les règles de sécurité et d'exploitation établies par l'AIFE, ainsi que les bonnes pratiques définies pour les environnements applicatifs. Toute exception fera l'objet d'un accord préalable écrit des équipes de l'AIFE.

Anti-virus opérationnel et à jour : le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation. La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée à l'acheteur.

Gestion des mises à jour : le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis à l'acheteur.

Sauvegarde des données : le titulaire met en place un système de sauvegarde permettant la sauvegarde des données de la prestation hébergées sur les serveurs du titulaire conformément aux besoins de sauvegarde exprimés par le chef de projet de l'acheteur dans le cadre de la Prestation. Des tests périodiques (a minima semestriels) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués.

Stockage des sauvegardes informatiques : le titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.

Comptes individuels : le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient

hébergées chez le titulaire ou chez l'acheteur) dispose d'un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au cours de la vie du compte

Comptes obsolètes ou par défaut : le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut d'usine devront être systématiquement modifiés.

Recensement des comptes d'accès : le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur existants ainsi que des rôles et privilèges qui y sont associés. Il fournit cette liste à l'acheteur sur demande. Le titulaire effectue et formalise une revue périodique des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation

Politique du moindre privilège : le titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège.

Attaques en essai et erreurs sur secrets d'authentification : les moyens d'authentification mis en place par le titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification

Journalisation des actions : le titulaire conserve de manière exploitable, sur une durée de 6 mois après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves. Ces activités devront s'appuyer sur une politique de gestion des journaux telle que celle publiée par l'ANSSI.

(Cf. <https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/>).

Le titulaire collecte et stocke à minima les informations suivantes :

- connexion et déconnexion aux équipements et applications ;
- consultations d'informations relatives à la vie privée ;
- informations d'usage de l'Internet (accès aux sites Web) ;
- accès en lecture et/ou en écriture à des fichiers et dossiers marqués « CONFIDENTIEL » ;
- informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du titulaire. Les traces enregistrées par le titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

Gestion des traces : le titulaire prévoit dans sa procédure de traitement d'incident un chapitre sur la préservation des traces éphémères (volatiles) en cas de suspicion d'attaque. Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être

journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, divers dates liées aux fichiers, clés de registres...). La procédure établit comment limiter l'activité susceptible de détruire ces traces éphémères.

Politique de mot de passe : le titulaire respecte la politique de définition des mots de passe de l'acheteur sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du titulaire.

Sources d'installation des logiciels : le titulaire dispose des sources d'installation des logiciels utilisés dans le cadre de la prestation, lorsque ces logiciels ne sont pas mis à disposition par l'acheteur.

Validité des licences : le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'acheteur dans le cadre de la prestation.

4.3.2.12 Cloisonnement des environnements et des rôles

Le titulaire a accès exclusivement aux environnements non productifs et utilise des données fictives.

Exceptionnellement, pour mener une investigation destinée à résoudre des dysfonctionnements, un accès à l'environnement de production sera autorisé de manière temporaire, ciblée et sur la base d'une demande argumentée. L'ouverture de l'accès dérogatoire n'est possible que ponctuellement sur instruction de l'AIFE à l'exploitant.

4.3.2.13 Traitement des incidents de sécurité

Remontée d'alerte : le service de supervision du titulaire met en place un système de remontée d'alerte à l'administration, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau), vol ou perte d'informations sensibles appartenant à l'administration (documentation technique en particulier).

Enregistrement et traçabilité et gestion des incidents de sécurité : le titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

Traitement des incidents de sécurité : le titulaire contacte les interlocuteurs sécurité de l'administration désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'acheteur. De plus :

- si cet incident a lieu sur le SI de l'acheteur, le titulaire participera à la demande de l'administration au traitement de l'incident ;
- si cet incident a lieu sur le SI du titulaire, le titulaire autorisera l'administration ou un tiers désigné à participer au traitement de l'incident.

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'administration (traitement des causes profondes).

4.3.2.14 Conformité, audit, inspection, contrôle

Autocontrôles de sécurité : le titulaire effectue des autocontrôles de conformité aux exigences des CCTP et PAS pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

Régularisation des écarts ou des non-conformités au niveau d'exigence de sécurité de l'acheteur : en cas de constatation d'écarts avec le CCTP ou le PAS et, plus généralement, en cas de non-conformité au niveau d'exigence de sécurité requis par l'acheteur, un plan de remédiation devra être formalisé par le titulaire 7 jours après la constatation des écarts. Le titulaire doit ensuite régulariser ces écarts par l'application du plan de remédiation dans un délai convenu en commun accord entre les deux parties.

4.3.2.15 Obligations spécifiques liées aux prestations de développement

Ségrégation des environnements : le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.

Protection des codes sources : le titulaire doit mettre en œuvre les mesures de sécurité nécessaires et adéquates à la protection des codes sources.

Il doit notamment contrôler systématiquement le code source généré par IA.

Le code source généré par IA doit faire l'objet de mesures de sécurité afin de vérifier son innocuité :

- proscrire l'exécution automatique de code source généré par IA dans l'environnement de développement ;
- proscrire le commit automatique de code source généré par IA dans les dépôts ;
- intégrer un outil d'assainissement de code source [3, 4] généré par IA dans l'environnement de développement ;
- vérifier l'innocuité des bibliothèques référencées dans le résultat du code source généré par IA ;
- faire contrôler régulièrement par un humain la qualité du code source généré à partir de requêtes types suffisamment sophistiquées.

La génération de code source par IA doit être limitée pour des modules critiques d'applications.

Il est fortement recommandé de ne pas utiliser un outil d'IA générative pour générer des blocs de code source destinés à des modules critiques d'applications :

- les modules de cryptographie (authentification, chiffrement, signature, etc.) ;
- les modules de gestion des droits d'accès des utilisateurs et administrateurs ;
- les modules de traitement de données sensibles.

Enfin, il est attendu que le code source généré par IA soit marqué.

Traçabilité des actions de développement : toute activité de développement doit être tracée et conservée dans un format facilitant son exploitation ultérieure.

Conduite des tests : lors de la conduite de tests de validation ou du déploiement, le titulaire doit :

- utiliser des données de tests anonymisées ;
- ne pas provoquer de perturbations du système d'information de l'acheteur lors des séances de test ;
- remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible
- ne pas introduire de régression vis-à-vis d'un état de sécurité atteint dans une version précédente

Contrôle de la qualité et de la sécurité du développement : l'administration se réserve le droit de contrôler la qualité et la sécurité du développement fourni par le titulaire, via des audits et/ou des tests d'intrusion par exemple (audit de code sur les parties les plus sensibles, etc.).

4.3.2.16 *Validation des modifications d'éléments d'architecture liés à la sécurité*

Un quelconque changement sur une brique technique support d'une fonction de sécurité est soumis à la validation de l'AIFE, notamment :

- toute ouverture de flux est soumise à la validation de l'AIFE.
- tout changement de configuration sur une des infrastructures support (par ex : fichier de règles des pare-feu) est soumis à la validation de l'AIFE.
- toute modification du paramétrage des briques techniques composant le service de signature est soumise à validation de l'AIFE. Toute modification des politiques de signature est soumise à la validation de l'AIFE.
- toute modification des paramétrages de la politique d'horodatage est soumise à la validation de l'AIFE.
- toute intégration d'une nouvelle IGC sur le système d'information est du ressort de l'AIFE.
- toute modification des politiques de validation de certificats est du ressort de l'AIFE.

4.3.2.17 *Middleware*

L'objectif est de renforcer la sécurité de la couche middleware en mettant en place des actions correctrices et préventives pour répondre aux exigences de conformité (RGPD, ISO 27001, etc.) :

- mise en place de politiques de sécurité adaptées pour chaque composant middleware ;
- mise en place de solutions et adaptations nécessaires pour corriger les vulnérabilités détectées suite à un audit de sécurité ou pour répondre aux évolutions des normes.

4.3.3 Sécurité liée aux ressources humaines

4.3.3.1 Gestion des ressources humaines

Chaque titulaire fournit une liste actualisée en permanence des personnels autorisés à intervenir sur le système, ainsi que leur niveau d'autorisation (types d'accès et ressources concernées) et leur périmètre d'activité.

4.3.3.2 Obligation de discrétion

Le personnel de chaque titulaire appelé à exécuter les prestations dans le cadre de son marché est tenu à une obligation de discrétion à l'égard de tous faits, informations ou documents dont il peut avoir connaissance lors de l'exécution du marché.

Chaque salarié, y compris les salariés d'éventuels sous-traitants, s'engage sur l'honneur à ne faire, ni pendant, ni après l'exécution du marché, aucune communication écrite ou verbale concernant toutes informations confidentielles dont il pourrait avoir connaissance à l'occasion de l'exécution du marché.

Tout manquement aux obligations de discrétion et de confidentialité est susceptible de tomber sous le coup de l'article 226-13 du code pénal et de l'article 50 de la loi 78-17 du 6 janvier 1978 (loi relative à l'informatique, aux fichiers et aux libertés).

Les titulaires sont responsables de l'application du respect de cette clause en ce qui concerne leurs éventuels sous-traitants.

Enfin, les obligations de discrétion et de confidentialité du présent article s'étendent 5 ans au-delà de la date de fin de marché.

En cas de violation par le titulaire des obligations de confidentialité mentionnées ci-dessus, et indépendamment des sanctions pénales éventuellement encourues, l'AIFE peut également résilier le marché aux torts du titulaire, sans mise en demeure préalable.

4.3.3.3 Engagement de confidentialité

Chaque titulaire s'engage à faire signer par tout personnel appelé à travailler à titre quelconque dans le cadre du présent cahier des charges l'« engagement de confidentialité des titulaires de marché » ainsi que la « charte utilisateurs pour l'usage des ressources informatiques et des services internet au sein de L'AIFE » propres à l'AIFE.

Chaque titulaire s'assure également que les personnels quittant le projet respectent la procédure de sortie de l'AIFE (restitution du matériel, des badges, fermeture des comptes, etc.) et ne détiennent plus de documents relatifs aux SI de la Commande publique.

4.3.3.4 Sous-traitance

Si un titulaire fait appel à une sous-traitance, celle-ci devra respecter l'ensemble des clauses de sécurité présentes dans ce document.

Par ailleurs, il est attendu de chaque titulaire que :

- La nature contractuelle des relations qui les unissent soient précisées ;
- Les conséquences en termes de responsabilité soient explicitées.

En cas de sous-traitance, chaque titulaire doit s'assurer qu'aucune messagerie autre que celle autorisée dans le cadre du projet et mise à disposition par l'AIFE n'est utilisée

pour tout ce qui concerne les activités de sa responsabilité au titre du présent accord-cadre et des marchés subséquents liés.

4.3.3.5 Contrôles de l'AIFE

Dans le cadre de l'exécution de chaque lot, l'AIFE se réserve le droit de réaliser des contrôles sur les personnels de chaque titulaire et des sous-traitants éventuels devant intervenir sur les systèmes d'information de la Commande publique.

4.3.3.5.1 Audits

L'AIFE peut, si elle le souhaite, réaliser ou faire réaliser des audits des prestations fournies par le Titulaire. Ceux-ci peuvent porter notamment sur les processus, l'organisation ou des aspects techniques :

- Audit de code source ;
- Audit de configuration ;
- Audit d'architecture ;
- Audit organisationnel ;
- Audit de site.

L'administration se réserve le droit de requérir l'expertise d'un organisme ou d'une société tierce présentant des compétences en matière de sécurité. Dans tous les cas, l'audit respectera la législation et la réglementation en vigueur sur le territoire français.

Les résultats de cette évaluation sont fournis à chaque titulaire concerné par l'AIFE afin qu'il propose et mette en œuvre les actions requises sur les non-conformités et points d'amélioration identifiés. Les plans d'actions et l'efficacité des actions implémentées sont validés par l'AIFE.

Pour toute vulnérabilité identifiée comme critique par l'auditeur et validée comme telle par l'AIFE, les titulaires doivent apporter un correctif définitif ou un contournement dans l'environnement de production dans le délai défini dans les indicateurs de service de chaque lot.

Le plan d'action de mise en conformité doit être fourni à l'AIFE par les Titulaires dans un délai de **7 jours calendaires** à compter de la réunion de restitution de l'audit.

4.3.3.5.1.1 Audit sécurité du code source

L'audit de code source consiste en l'analyse de tout ou partie du code source d'une application dans le but d'y découvrir des vulnérabilités, liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en termes de sécurité.

L'audit vérifie, a minima, la sécurité des parties du code source relatives à :

- l'authentification ;
- la gestion des utilisateurs et de leurs habilitations ;
- le contrôle d'accès aux ressources ;
- les interactions avec d'autres applications ;

- les relations avec les systèmes de gestion de bases de données ;
- la conformité aux exigences de sécurité relative à l'environnement dans laquelle l'application est déployée.

Les audits de code source peuvent être réalisés manuellement ou automatiquement par des outils spécialisés.

4.3.3.5.1.2 Audit de configuration

L'audit de configuration a pour vocation de vérifier la mise en œuvre des bonnes pratiques de sécurité dans la configuration des dispositifs matériels et logiciels déployés dans un système d'information. Ces dispositifs peuvent notamment être des équipements réseau, des produits de sécurité, des serveurs, des systèmes d'exploitation ou des applications.

L'audit vérifiera, à minima, la sécurité des configurations :

- des équipements réseau de type commutateurs ou routeurs (règles de filtrage et de configuration de VLAN par exemple),
- des équipements de sécurité de type pare-feux ou relais inverse (filtrant ou non) et leurs règles de filtrage,
- des systèmes d'exploitation,
- des systèmes de gestion de bases de données,
- des services réseau classiques : SSH, HTTP, SMTP, DNS, etc.
- des serveurs d'applications : JBoss, Apache Tomcat, IBM Websphere, etc.
- des environnements de virtualisation.

4.3.3.5.1.3 Audit d'architecture

L'audit d'architecture consiste en la vérification de la prise en compte des bonnes pratiques de sécurité relatives au choix, au positionnement, au déploiement et à la mise en œuvre des dispositifs matériel et logiciels déployés dans un système d'information. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

L'audit procédera à la revue des documents suivants :

- schémas d'architectures de niveau 2 et 3 du modèle OSI,
- matrices de flux,
- règles de filtrage,
- configuration des équipements réseau (routeurs et commutateurs),
- interconnexions avec des réseaux tiers ou Internet,
- documents d'architecture technique liés à la cible.

4.3.3.5.1.4 Audit organisationnel

L'audit de l'organisation de la sécurité vise à s'assurer que les politiques et procédures de sécurité définies par l'audité, pour assurer le maintien en conditions opérationnelles et de sécurité d'une application ou de tout ou partie du système d'information :

- sont conformes au besoin de sécurité du titulaire, à l'état de l'art ou aux normes en vigueur,
- complètent correctement les mesures techniques mises en place,
- sont mises en pratique.

4.3.3.5.1.5 Audit de la sécurité physique des locaux

Le principe de l'audit de sécurité physique des locaux est de contrôler que l'ensemble des dispositions pour préserver le matériel socle du système d'information ont été prises.

L'audit vérifiera, a minima, la sécurité des locaux à travers :

- la gestion des accès physiques aux locaux,
- la télésurveillance des locaux,
- la sécurisation des bureaux, des salles et des équipements, zonage,
- les mécanismes de continuité d'activité (gestion des pannes d'électricité, catastrophes naturelles, ...),
- les choix de l'emplacement et protection du matériel,
- la bonne maintenance du matériel.

4.3.3.5.1.6 Corrections des failles de sécurité

Les failles de sécurité sont constituées des vulnérabilités des composants du système d'information et de celles liées au développement et au paramétrage, notamment découvertes lors d'un audit.

Le Titulaire maintient une veille sur les vulnérabilités, via le CERT-FR, les fournisseurs de solutions logicielles, ses propres services, etc.

Il applique les correctifs dans un délai maximum de 1 mois.

En cas d'alerte grave (exploitation avérée d'une faille critique, faille critique, injonction de l'ANSSI), le correctif doit être appliqué dans un délai de 24 heures avec une priorité sur les environnements productifs.

Lorsqu'aucun correctif n'est disponible, le Titulaire doit suivre les recommandations de l'éditeur ou du CERT- FR dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le Titulaire s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

4.4 Exigences en matière de ressources humaines

Le titulaire s'engage sur la stabilité, la disponibilité et la montée en compétences des équipes affectées :

- Chaque profil mobilisé fait l'objet d'un CV validé en amont par l'AIFE ; tout remplacement doit être proposé avec un profil équivalent ou supérieur ;
- Le titulaire garantit une couverture de présence sur site de 3 jours par semaine à minima ;
- Les intervenants maîtrisent la langue française, à l'écrit comme à l'oral ;
- Un plan de maintien des compétences (veille, formations, certifications) est partagé annuellement.

4.5 Exigences de qualité logicielle et de niveaux de service (Lot 2)

Sur le périmètre front-end du Lot 2, le titulaire s'engage *a minima* sur les seuils suivants, mesurés sur les livrables intégrés au RCN :

- Couverture de tests unitaires ≥ 80 % sur les composants ;
- Zéro erreur critique lint/ESLint sur le code livré ;
- Core Web Vitals respectés sur les écrans livrés (LCP < 2,5 s, CLS < 0,1, INP < 200 ms sur profil de référence AIFE) ;
- Taux de régression post-livraison < 5 % (anomalies bloquantes ou majeures détectées dans les 30 jours suivant la mise en production).

Tout dépassement donne lieu à un plan d'actions correctives. Des pénalités peuvent être appliquées conformément au CCAP.

4.6 Exigences méthodologiques et d'industrialisation

Le titulaire adopte les pratiques et l'outillage de l'AIFE :

- Méthode agile (sprints de 2 semaines, cérémonies Scrum) pour la conduite des bons de commande ;
- Outils de gestion : GitLab (code + CI/CD), Figma Enterprise (maquettes), Storybook (documentation de composants) ;
- Respect des conventions de commit, des règles de branching et des gabarits de Pull Request définis par l'AIFE ;
- Participation aux communautés de pratique (UX, front-end) animées par l'AIFE.

Aucun outil externe non validé par l'AIFE ne peut être introduit dans la chaîne de production.

4.7 Exigences de traçabilité et de gouvernance

Chaque décision structurante (choix de conception, arbitrage RCN, migration technique, dérogation) est documentée et tracée dans un Architecture Decision Record (ADR) ou équivalent, stocké dans l'outil fourni par l'AIFE. Le titulaire tient à jour :

- Le registre des évolutions par bon de commande ;
- Le registre des anomalies et des dérogations ;
- Le journal des accès aux environnements de production (Lot 2).

Ces registres sont consultables à tout moment par l'AIFE et versés à la clôture de chaque bon de commande.

4.8 Exigences relatives à la relation avec des tiers

L'AIFE mobilise plusieurs prestataires sur l'écosystème numérique (MOA métier, autres MOE, exploitants, SN1/SN2, équipe sécurité). Le titulaire :

- Coopère activement avec les autres titulaires et les équipes internes AIFE dans un esprit de transparence et de co-construction ;
- Participe aux comités de coordination inter-prestataires lorsqu'ils sont organisés ;
- N'entre pas en conflit d'intérêts avec des prestataires en charge de la TMA ou de l'exploitation des applications concernées ;
- Informe sans délai l'AIFE de toute difficulté de collaboration avec un tiers.

4.9 Exigences de transférabilité et de réversibilité

À l'expiration ou à la résiliation du marché, le titulaire assure :

- La transférabilité : tous les livrables, codes sources, maquettes, documentations, plans de marquage et ADR sont remis à l'AIFE dans un format exploitable et documenté ;
- La réversibilité : un plan de réversibilité est produit dans les 3 mois précédant le terme de l'accord-cadre, couvrant la reprise par l'AIFE ou par un titulaire successeur (transfert de connaissances, sessions de passation, période de double présence si applicable) ;
- Le maintien en condition de réversibilité sur toute la durée du marché : le titulaire documente en continu ses productions pour qu'elles soient reprises à tout moment sans dépendance au personnel du titulaire.

La réversibilité est mise en œuvre à titre gracieux jusqu'à 15 jours ouvrés cumulés ; au-delà, elle est valorisée sur la base des UO du marché.

4.10 Exigences d'amélioration continue

Le titulaire contribue activement à l'amélioration continue des pratiques de l'AIFE :

- Il propose, a minima annuellement, un plan de progrès (simplification, mutualisation, innovation) soumis au comité de pilotage ;
- Il partage les retours d'expérience post-livraison (REX) dans un format standardisé AIFE ;
- Il alimente les bilans quantitatifs et qualitatifs produits par l'AIFE pour le pilotage du marché ;
- Il s'engage sur des objectifs d'écoconception et de sobriété numérique (optimisation des bundles, des images, des requêtes réseau).

Ces engagements sont suivis via des indicateurs partagés au comité de pilotage.

5 LOT 1 — ASSISTANCE À MAÎTRISE D'OUVRAGE EN UX/UI

5.1 Objet et périmètre du Lot 1

L'AIFE souhaite disposer de prestations d'assistance à maîtrise d'ouvrage (AMOA) spécialisées en conception UX/UI pour concevoir, piloter et faire évoluer l'expérience utilisateur de ses projets numériques. Le titulaire intervient en amont des développements et en coordination avec les équipes MOA et MOE, sur l'ensemble du cycle de conception.

Les prestations sont structurées en cinq Unités d'Œuvre (UO), chacune déclinée en quatre niveaux de complexité.

5.2 Modalités d'exécution du Lot 1

5.2.1 Lieu d'exécution et outils

Des déplacements en région parisienne peuvent être requis pour les ateliers et tests. Le titulaire travaille dans l'environnement Figma de l'AIFE et utilise les outils de gestion de projet (Jira, Confluence ou équivalents).

5.2.2 Délais d'intervention

- Démarrage d'une mission : au plus tard 5 jours ouvrés après notification du bon de commande ;
- Remise de tout livrable : selon le planning validé en réunion de lancement.

5.3 Unités d'œuvre du Lot 1

5.3.1 L1-UX-P1 — Cadrage & Discovery

Objet : Recueillir les besoins, cadrer la démarche UX/fonctionnelle et définir les parcours cibles en assurant l'alignement initial avec le RCN et les besoins de mesure.

Prestations incluses :

- Animation d'un ou plusieurs ateliers de recueil des besoins (métier et utilisateurs) et formalisation des décisions.
- Production d'une note de cadrage UX/fonctionnelle : objectifs, périmètre, contraintes, hypothèses, priorités.
- Cartographie d'un ou plusieurs parcours utilisateurs (user journey), identification des irritants et opportunités.
- Préconisations initiales relatives à l'alignement RCN (composants/patterns mobilisables, écarts pressentis).
- Identification des événements clés à mesurer sur les parcours (premières recommandations analytics).

Livrables attendus :

- Compte-rendu d'ateliers.
- Note de cadrage UX/fonctionnelle et backlog macro (parcours / écrans / US).
- Cartographie des parcours et synthèse des points de mesure.

Conditions d'acceptation : Livrables complets, traçant les décisions et hypothèses. Validation par la MOA et partage à la MOE.

Profils indicatifs : UX Designer, UX Researcher, Facilitateur d'ateliers

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L1-UX-P1	Cadrage & Discovery	Simple	1 à 2 ateliers, périmètre restreint (1 parcours, < 5 écrans), contexte métier connu, peu de parties prenantes	3 – 5 j.o.
		Moyen	2 à 4 ateliers, 1 à 3 parcours (5 à 15 écrans), quelques contraintes RCN, 3 à 5 parties prenantes	5 – 8 j.o.
		Complexe	4 à 6 ateliers, multi-parcours (15 à 30 écrans), contraintes RCN avérées, parties prenantes nombreuses ou contexte métier complexe	8 – 15 j.o.
		Très complexe	Plus de 6 ateliers, multi-service ou multi-périmètre (> 30 écrans), fortes contraintes d'intégration, nombreuses équipes mobilisées	15 – 25 j.o.

5.3.2 L1-UX-P2 — Conception & Prototypage

Objet : Concevoir l'expérience et produire des maquettes/prototypes exploitables par la MOE, conformes au RCN et intégrant accessibilité et besoins de mesure.

Prestations incluses :

- Ateliers de co-conception et itérations de conception.
- Production de wireframes et maquettes Figma en cohérence avec le RCN.
- Définition des comportements et états (chargement, erreur, vide, succès), règles de contenu et cas limites.
- Rédaction de spécifications orientées usages : user stories, critères d'acceptation, règles UX/UI.
- Formalisation des recommandations analytics : mapping parcours/écrans → événements, propriétés, règles de déclenchement.

Livrables attendus :

- Maquettes Figma (wireframes et/ou haute fidélité) et prototype cliquable.
- Annotations et spécifications (US + critères d'acceptation + règles UX/UI).
- Fiche de recommandations analytics (événements/propriétés) liée au parcours.

Conditions d'acceptation : Maquettes et prototypes exploitables pour intégration. Conformité au RCN ou écarts explicités et arbitrés. Recommandations analytics cohérentes avec les objectifs projet.

Profils indicatifs : UX Designer, UI Designer, Product Designer

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L1-UX-P2	Conception & Prototypage	Simple	1 parcours, < 5 écrans, composants RCN existants, peu d'états, 1 à 2 itérations	4 – 7 j.o.
		Moyen	1 à 2 parcours, 5 à 15 écrans, quelques composants à adapter, états multiples, 2 à 3 itérations	8 – 15 j.o.
		Complexe	Multi-parcours, 15 à 30 écrans, nouveaux composants à créer, responsive exigeant, 3 à 5 itérations	15 – 25 j.o.
		Très complexe	Service complet, > 30 écrans, nombreux nouveaux patterns, contraintes d'accessibilité étendues, nombreuses itérations et parties prenantes	25 – 45 j.o.

5.3.3 L1-UX-P3 — Tests utilisateurs

Objet : Valider et itérer les maquettages et/ou un POC codé par des tests utilisateurs, afin d'objectiver les choix de conception et prioriser les améliorations.

Prestations incluses :

- Définition du protocole (objectifs, hypothèses, scénarios, critères d'observation).
- Préparation des supports de test : prototype Figma et/ou environnement de test / POC codé.
- Organisation et conduite des sessions (modérées, distanciel/présentiel selon bon de commande).
- Analyse des résultats : irritants, causes racines, recommandations.
- Restitution et mise à jour du backlog / des livrables UX (selon périmètre du bon de commande).

Livrables attendus :

- Protocole de test + scénarios.
- Synthèse des résultats (irritants priorisés, recommandations, verbatims synthétiques).
- Plan d'actions / backlog de corrections.
- Le cas échéant : version amendée des maquettes/prototypes.

Conditions d'acceptation : Livrables actionnables (priorisation, recommandations concrètes, traçabilité). Restitution réalisée auprès de la MOA et partagée à la MOE.

Profils indicatifs : UX Researcher, Chargé de recherche utilisateur, UX Designer

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L1-UX-P3	Tests utilisateurs	Simple	3 à 5 participants, 1 parcours, sessions distancielles, protocole standardisé, synthèse légère	3 – 5 j.o.
		Moyen	5 à 8 participants, 1 à 2 parcours, mixte distanciel/présentiel, analyse approfondie	5 – 10 j.o.
		Complexe	8 à 12 participants, multi-parcours, profils diversifiés (dont personnes en situation de handicap), plusieurs cycles de tests	10 – 18 j.o.
		Très complexe	> 12 participants, service complet, profils très variés, tests sur POC codé, itérations multiples avec mise à jour des maquettes incluse	18 – 30 j.o.

5.3.4 L1-UX-P4 — Validation & Recette UX/UI

Objet : Préparer et conduire la recette UX/UI des évolutions, vérifier la conformité aux intentions UX/UI et au RCN, et contrôler la prise en compte des recommandations analytics.

Prestations incluses :

- Définition de la stratégie et des scénarios de recette UX/UI (checklists, critères).
- Exécution de la recette : constats, création et priorisation des anomalies, retests.
- Vérification de cohérence UI et conformité aux principes RCN.
- Vérification fonctionnelle des recommandations analytics (présence/pertinence des déclenchements, cohérence des propriétés) sur le périmètre du bon de commande.

Livrables attendus :

- Cahier de recette UX/UI.
- Procès-verbal de recette (PV) et liste d'anomalies priorisées.
- Synthèse de vérification analytics (périmètre, constats, écarts).

Conditions d'acceptation : PV de recette établi et partagé à la MOA/MOE. Anomalies qualifiées et priorisées de manière actionnable.

Profils indicatifs : UX Designer, UI Designer, Chargé de recette UX

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L1-UX-P4	Validation & Recette UX/UI	Simple	< 5 écrans ou évolutions mineures, critères de recette standards, 1 cycle de tests/retests	2 – 4 j.o.
		Moyen	5 à 15 écrans, recette fonctionnelle et conformité RCN, 1 à 2 cycles de tests/retests	4 – 8 j.o.
		Complexe	15 à 30 écrans, vérification analytics intégrée, recette multi-navigateurs/terminaux, 2 à 3 cycles	8 – 15 j.o.
		Très complexe	> 30 écrans, service complet, recette exhaustive (fonctionnel + RCN + analytics + accessibilité), plusieurs cycles + régressions	15 – 25 j.o.

5.3.5 L1-UX-P5 — Suivi & Amélioration continue

Objet : Accompagner le produit après livraison, capitaliser les retours et proposer des améliorations UX/UI en continu, en cohérence avec le RCN.

Prestations incluses :

- Analyse des retours (support, utilisateurs, métiers) et identification des irritants.
- Proposition d'améliorations priorisées (quick wins et évolutions structurantes).
- Mise à jour des livrables UX (maquettes/prototypes/specs) lorsque nécessaire.
- Capitalisation des apprentissages (décisions, patterns, recommandations réutilisables).

Livrables attendus :

- Rapport de suivi (mensuel ou par sprint) et backlog d'amélioration priorisé.
- Éléments de capitalisation (notes de synthèse, recommandations, patterns).

Conditions d'acceptation : Livrables transmis dans les délais prévus au bon de commande. Backlog priorisé et exploitable par la MOA/MOE.

Profils indicatifs : UX Designer, Product Designer, UX Analyst

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L1-UX-P5	Suivi & Amélioration continue	Simple	Suivi mensuel léger, < 5 améliorations identifiées, mise à jour mineure de maquettes, 1 service	1 – 2 j.o. / mois
		Moyen	Suivi par sprint, 5 à 15 améliorations, quelques mises à jour Figma, 1 à 2 services	2 – 4 j.o. / sprint
		Complexe	Suivi multi-services, 15 à 30 améliorations, mise à jour de patterns RCN, capitalisation structurée	4 – 8 j.o. / sprint
		Très complexe	Programme d'amélioration continue multi-services, > 30 améliorations, contribution active au RCN, animation de communauté UX	8 – 15 j.o. / sprint

6 LOT 2 — ASSISTANCE À MAÎTRISE D'ŒUVRE UI / DÉVELOPPEMENT FRONT-END (RCN)

6.1 Objet et périmètre du Lot 2

L'AIFE souhaite confier des prestations de maîtrise d'œuvre (AMOE) portant sur le développement d'interfaces utilisateur conformes au RCN, l'industrialisation de la chaîne front-end et la mise en œuvre d'un cadre analytics robuste. Le titulaire intervient sur la librairie Angular du RCN ainsi que sur le renforcement des équipes de développement des projets applicatifs de l'AIFE, en mode agile et en coordination étroite avec la MOA/UX.

Les prestations sont structurées en cinq Unités d'Œuvre (UO), chacune déclinée en quatre niveaux de complexité.

6.2 Modalités d'exécution du Lot 2

6.2.1 Environnement technique

Le titulaire travaille dans l'environnement de l'AIFE : GitLab (versionnement et CI/CD), Angular CLI, Node.js, Storybook, ESLint, Prettier. L'accès aux outils est conditionné à la signature des accords de sécurité et confidentialité du CCAP.

6.2.2 Transfert de compétences

Pour tout bon de commande supérieur à trois (3) mois, le titulaire établit un plan de transfert de compétences garantissant la reprise en autonomie des livrables par les équipes AIFE.

6.2.3 Délais d'intervention

- Première mise à disposition d'un profil : au plus tard 10 jours ouvrés après émission du bon de commande ;

6.3 Unités d'œuvre du Lot 2

6.3.1 L2-DEV-P1 — Création/évolution de composant(s) UI RCN

Objet : Développer et livrer des composants UI Angular conformes au RCN, testés, accessibles (RGAA) et documentés dans Storybook.

Prestations incluses :

- Implémentation des maquettes validées par la MOA/UX sous forme de composants Angular réutilisables.
- Garantie de la conformité au RCN (tokens de design, variantes, états, responsive).
- Tests unitaires et tests d'accessibilité automatisés (axe-core ou équivalent).
- Documentation Storybook : stories, props, variantes, états, notice d'accessibilité.
- Contribution aux revues de code avec les équipes AIFE.

Livrables attendus :

- Composant(s) Angular livré(s) avec tests et code source.
- Documentation Storybook mise à jour.
- Rapport de couverture de tests et résultats d'accessibilité automatisée.

Conditions d'acceptation : Composants conformes au RCN, couverts par les tests, documentés et validés en revue de code avant merge.

Profils indicatifs : Développeur front-end Angular, Développeur UI, Intégrateur Angular

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L2-DEV-P1	Création/évolution de composant(s) UI RCN	Simple	1 composant basique, 1 à 2 variantes, états simples, composants Angular standards existants réutilisés	2 – 5 j.o.
		Moyen	1 à 3 composants, plusieurs variantes/états, interactions modérées, quelques nouvelles règles RCN	5 – 10 j.o.
		Complexe	3 à 6 composants interconnectés, animations, nombreux états/variantes, contraintes RGAA étendues	10 – 20 j.o.
		Très complexe	Système de composants (> 6), patterns avancés, orchestration de services, Design OPS intégré, rétrocompatibilité exigeante	20 – 40 j.o.

6.3.2 L2-DEV-P2 — Implémentation d'interfaces et d'écrans

Objet : Implémenter des interfaces complètes (pages ou ensembles d'écrans) à partir des maquettes Figma validées, en intégrant les composants de la librairie Angular RCN et en assurant la conformité RGAA. Le périmètre de connexion aux API back-end est défini au bon de commande : certaines missions couvrent uniquement l'intégration UI (avec données mockées), d'autres incluent la connexion aux API réelles.

Prestations incluses :

- Intégration fidèle des maquettes Figma en composants Angular issus de la librairie RCN.
- Gestion des états d'interface (chargement, erreur, vide, succès) avec données mockées ou connectées selon périmètre du bon de commande.
- Connexion aux API back-end et gestion des états applicatifs réels (si inclus au bon de commande).
- Prise en charge des cas limites et des interactions complexes.
- Tests unitaires et, selon périmètre, tests d'intégration et/ou end-to-end sur les parcours implémentés.
- Coordination avec la MOA/UX pour les ajustements de mise en œuvre, dans le cadre des sprints de 2 semaines.

Livrables attendus :

- Interfaces développées, testées et intégrées dans le dépôt GitLab.
- Rapport de tests (unitaires et/ou intégration selon périmètre).
- Fiche de mise en œuvre (écarts maquettes / implémentation, justifications, périmètre API couvert).

Conditions d'acceptation : Interfaces conformes aux maquettes Figma et à la librairie Angular RCN, couvertes par les tests définis au bon de commande, validées en Sprint Review ou en recette MOA/UX.

Profils indicatifs : Développeur front-end Angular, Développeur front-end, Développeur full-stack front

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L2-DEV-P2	Implémentation d'interfaces et d'écrans	Simple	1 à 3 écrans, interactions simples, données mockées uniquement, composants RCN existants, peu de cas d'erreur	3 – 7 j.o.
		Moyen	3 à 10 écrans, formulaires et validations, gestion d'états complète (mock ou API simple), responsive standard	7 – 18 j.o.

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
		Complexe	10 à 20 écrans, parcours complet, gestion d'état avancée, connexion API (si incluse), accessibilité exigeante, multi-navigateurs	18 – 35 j.o.
		Très complexe	> 20 écrans, service complet, connexion multi-API, gestion d'état avancée (NgRx ou équivalent), optimisations performances, full RGAA	35 – 60 j.o.

6.3.3 L2-DEV-P3 — Expertise architecture & gouvernance front-end

Objet : Définir et documenter l'architecture front-end des projets, la stratégie de versioning, les préconisations CI/CD et les recommandations d'infrastructure serveur, en cohérence avec le RCN et l'environnement technique de l'AIFE. Le titulaire intervient exclusivement en conseil et en cadrage ; la mise en œuvre opérationnelle relève du socle technique de l'AIFE.

Prestations incluses :

- Audit et analyse de l'architecture front-end existante (structure, dépendances, couplages).
- Définition de la stratégie de versioning (SemVer, politique de branches, gestion des dépendances inter-projets).
- Préconisations CI/CD : pipeline de build, tests automatisés, publication de librairie, sans mise en œuvre opérationnelle.
- Recommandations d'infrastructure serveur : environnements (dev / recette / prod), stratégie de build et optimisation des bundles.
- Cadrage de la gouvernance front-end : conventions de code, procédures de revue, standards de documentation technique.

Livrables attendus :

- Note d'architecture front-end (état des lieux, préconisations, arbitrages).
- Stratégie de versioning et politique de branches documentée.
- Préconisations CI/CD et infrastructure (document de recommandations argumenté).
- Guide de gouvernance front-end (conventions, procédures, standards de documentation technique).

Conditions d'acceptation : Livrables directement actionnables par les équipes AIFE et le socle technique. Recommandations argumentées, priorisées et cohérentes avec l'environnement existant. Traçabilité des décisions et arbitrages.

Profils indicatifs : Architecte front-end, Expert Angular, Tech Lead front-end

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L2-DEV-P3	Expertise architecture & gouvernance front-end	Simple	Cadrage d'architecture sur 1 projet front-end, stratégie de versioning initiale, premières préconisations CI/CD et d'infrastructure	1 – 3 j.o.
		Moyen	Architecture de 2 à 3 projets interconnectés, stratégie multi-dépôts, recommandations CI/CD et d'infrastructure sur 1 environnement	3 – 8 j.o.
		Complexe	Architecture d'un écosystème complet (bibliothèque + applications), gouvernance multi-équipes, recommandations CI/CD et infrastructure multi-environnements	8 – 18 j.o.
		Très complexe	Refonte architecturale de l'écosystème RCN, stratégie de déploiement multi-environnements, gouvernance technique inter-projets et coordination multi-marchés	18 – 35 j.o.

6.3.4 L2-DEV-P4 — Analytics & Plan de marquage

Objet : Définir et mettre en œuvre le cadre de collecte de données (plan de marquage, nomenclature, gouvernance) et industrialiser la mesure pour fiabiliser le pilotage par la donnée.

Prestations incluses :

- Définition du plan de marquage : parcours/écrans → événements, propriétés, règles de déclenchement.
- Implémentation des événements analytics dans le code front-end.
- Mise en place de tests de non-régression analytics (vérification de la présence et de la cohérence des déclenchements).
- Documentation du plan de marquage et des règles de gouvernance.
- Contrôle qualité des données en lien avec les équipes data de l'AIFE.

Livrables attendus :

- Plan de marquage documenté (tableur ou outil dédié).
- Implémentation des événements dans le code source.
- Rapport de tests de non-régression analytics.
- Guide de gouvernance analytics.

Conditions d'acceptation : Plan de marquage validé par la MOA. Événements déclenchés correctement, vérifiés par tests automatisés ou manuels.

Profils indicatifs : Développeur front-end Angular, Développeur front-end, Ingénieur analytics / tracking

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L2-DEV-P4	Analytics & Plan de marquage	Simple	< 10 événements, 1 parcours, implémentation sur composants existants, vérification manuelle	2 – 4 j.o.
		Moyen	10 à 30 événements, 1 à 2 parcours, plan de marquage formalisé, tests manuels + automatisés partiels	4 – 10 j.o.
		Complexe	30 à 80 événements, multi-parcours, gouvernance définie, tests automatisés complets, revue avec équipes data	10 – 20 j.o.
		Très complexe	> 80 événements, framework analytics complet, non-régression systématique, tableaux de bord de suivi qualité données, plusieurs équipes	20 – 40 j.o.

6.3.5 L2-DEV-P5 — Expertise & accompagnement en maintenance front-end

Objet : Apporter une expertise technique front-end en appui des équipes en charge de la maintenance et de l'évolution des composants RCN et des interfaces livrées, afin de sécuriser les choix techniques et de préserver, dans la durée, la conformité au RCN et au RGAA. Le titulaire n'assure pas la réalisation opérationnelle des correctifs ; il intervient en conseil, cadrage et revue.

Prestations incluses :

- Revue d'architecture et diagnostic technique sur les composants RCN et interfaces en production (revue de code, audit ciblé, analyse de causes racines d'anomalies complexes).
- Conseil sur les stratégies de mise à jour liées aux évolutions du RCN ou aux montées de version Angular : analyse d'impact, plan de migration, arbitrages de rétrocompatibilité.
- Préconisations de refactoring et d'optimisation (dette technique, performance, accessibilité) — rédaction des orientations, sans mise en œuvre directe.
- Cadrage et relecture des mises à jour de documentation Storybook et des guides de contribution produits par les équipes de réalisation.
- Conseil en gestion des dépendances et des alertes de sécurité front-end : analyse des CVE, qualification du risque, recommandations de remédiation.
- Appui ponctuel sur incidents ou arbitrages complexes : expertise de second niveau, pair-programming, revue de Pull Requests, sans prise en charge opérationnelle de la correction.

Livrables attendus :

- Notes d'expertise / de diagnostic (constats, analyses, recommandations priorisées).
- Rapports d'audit technique ou de revue de code avec plan d'actions.
- Avis techniques documentés (migrations, dépendances, sécurité).
- Comptes rendus des sessions d'accompagnement (revues, ateliers, pair-programming).

Conditions d'acceptation : Livrables d'expertise directement actionnables par les équipes AIFE, argumentés et hiérarchisés. Traçabilité des recommandations et des arbitrages.

Profils indicatifs : Architecte front-end, Expert Angular, Tech Lead front-end

Niveaux de complexité :

Code UO	Libellé	Complexité	Critères / Périmètre indicatif	Délai indicatif (j.o.)
L2-DEV-P5	Expertise & accompagnement en maintenance front-end	Simple	Diagnostic ciblé sur 1 à 2 composants, revue de code ponctuelle, avis technique sur une dépendance ou une alerte de sécurité	1 – 3 j.o.
		Moyen	Analyse d'impact sur 3 à 8 composants, préconisations de migration Angular mineure, revue de Pull Requests, qualification d'anomalies complexes	3 – 8 j.o.
		Complexe	Audit technique multi-composants (> 8), plan de migration Angular majeure, arbitrages de rétrocompatibilité, accompagnement sur incidents complexes	8 – 20 j.o.
		Très complexe	Expertise architecturale complète de la librairie, accompagnement d'une migration technologique majeure (> 20 composants), gouvernance front-end multi-équipes	20 – 45 j.o.