

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)

N° DGFIP-DRS-2500030 du 23/09/2025

**Fourniture de prestations d'assistance relatives à l'urbanisation,
l'architecture applicative et la sécurité du système d'information de la
DGFIP**

Procédure de marché : appel d'offres ouvert

Table des matières

1	Présentation générale de la consultation.....	6
1.1	Objet du marché.....	6
1.2	Allotissement.....	6
1.3	Présentation de la DGFiP.....	7
1.4	Structures de la DGFiP.....	7
1.5	Le SI DGFiP en 2025.....	10
1.5.1	Des agents au cœur du système d'information.....	10
1.5.2	Une organisation qui a évolué.....	10
1.5.3	Des projets au service du système d'information.....	10
1.5.4	Des technologies et une méthode.....	10
1.6	Les grands principes directeurs du SI de la DGFiP.....	10
1.7	Pilotage global du marché.....	12
1.7.1	Le comité de pilotage.....	12
1.7.2	Le comité de suivi.....	12
1.8	Description des unités d'œuvre (UO).....	13
1.9	Exigences communes aux trois lots.....	13
1.10	Exigences qualité associées aux prestations.....	15
1.10.1	Garantie de qualifications minimales et de stabilité pour les intervenants.....	15
1.10.2	Niveaux de service et pénalités.....	21
*	La non-conformité sera évaluée par l'administration lors d'un entretien.....	22
1.10.3	Qualité des livrables.....	22
2	Contexte d'exécution du marché.....	23
2.1	Présentation des réalisations d'études d'urbanisation (lot 1).....	24
2.2	Présentation des instructions d'architecture (lot 2).....	26
2.2.1	Les instructions CAI.....	26
2.2.1.1	Le Dossier d'Architecture Générale et Détaillée (DAGD).....	29
2.2.2	Les instructions FQE.....	30
2.2.3	Les instructions d'architecture fonctionnelle.....	30
2.3	Présentation du lot 3.....	31
2.3.1	Présentation de la démarche d'intégration de la sécurité dans les projets (ISP).....	31
2.3.2	Présentation de la procédure d'étude d'impact sur la vie privée à la DGFiP.....	33
3	Présentation du méta-modèle de la DGFiP.....	36
4	Explication sur le cas d'utilisation.....	37
5	Présentation des unités d'œuvre (UO) du lot 1.....	37
5.1	Unités d'œuvre du lot 1.....	37
5.1.1	UO PRC - Prise de Connaissance.....	37
5.1.1.1	Contenu de la prestation.....	37
5.1.1.2	Fournitures de l'administration.....	38
5.1.1.3	Livrables de la prestation.....	38
5.1.1.4	Personnels du titulaire concernés.....	38
5.1.1.5	Niveau de complexité et délai de réalisation minimum.....	38
5.1.2	UO RTC - Réversibilité, Transfert de Compétences.....	38
5.1.2.1	Contenu de la prestation.....	38
5.1.2.2	Fournitures de l'administration.....	38

5.1.2.3	Livrables de la prestation.....	39
5.1.2.4	Compétences recherchées.....	39
5.1.2.5	Niveau de complexité et délai de réalisation minimum.....	39
5.1.3	UO Urbanisation (URB).....	39
5.1.3.1	Contenu de la prestation.....	39
5.1.3.2	Fournitures de l'administration.....	40
5.1.3.3	Livrables de la prestation.....	40
5.1.3.4	Compétences recherchées.....	42
5.1.3.5	Niveau de complexité et <i>délai de réalisation minimum</i>	42
5.1.4	UO Cartographie (CTO).....	45
6	Présentation des unités d'œuvre (UO) communes aux 2 lots (2 et 3).....	46
6.1	UO PRC - PRise de Connaissance.....	46
6.1.1	Contenu de la prestation.....	46
6.1.2	Fournitures de l'administration.....	46
6.1.3	Livrables de la prestation.....	47
6.1.4	Compétences recherchées.....	47
6.1.5	Niveau de complexité et délai de réalisation minimum.....	47
6.2	UO RTC - Réversibilité, Transfert de Compétence.....	47
6.2.1	Contenu de la prestation.....	47
6.2.2	Fournitures de l'administration.....	47
6.2.3	Livrables de la prestation.....	47
6.2.4	Compétences recherchées.....	48
6.2.5	Niveau de complexité et délai de réalisation minimum.....	48
7	Présentation des unités d'œuvre (UO) du lot 2.....	48
7.1	UO EPA - Expertise Ponctuelle d'Architecture.....	48
7.1.1	Contenu de la prestation.....	48
7.1.2	Fournitures de l'administration.....	49
7.1.3	Livrables de la prestation.....	49
7.1.4	Compétences recherchées.....	49
7.1.5	Niveau de complexité et délai de réalisation minimum.....	50
7.2	UO ECE - Étude de Cohérence et d'Évaluation de la trajectoire de migration du SI.....	50
7.2.1	Contenu de la prestation.....	50
7.2.2	Fournitures de l'administration.....	50
7.2.3	Livrables de la prestation.....	51
7.2.4	Compétences recherchées.....	51
7.2.5	Niveau de complexité et délai de réalisation minimum.....	51
7.3	UO CPP - Conseils et Promotion aux Projets.....	52
7.3.1	Contenu de la prestation.....	52
7.3.2	Fournitures de l'administration.....	52
7.3.3	Livrables de la prestation.....	52
7.3.4	Compétences recherchées.....	52
7.3.5	Niveau de complexité et délai de réalisation minimum.....	53
7.4	UO IAP - Instructions d'Architecture des Projets.....	53
7.4.1	Contenu de la prestation.....	53
7.4.2	Fournitures de l'administration.....	53
7.4.3	Livrables de la prestation.....	54
7.4.4	Compétences recherchées.....	54

7.4.5 Niveau de complexité et délai de réalisation minimum.....	55
7.5 UO MCA - Mise à jour du Cadre d'Architecture applicative.....	56
7.5.1 Contenu de la prestation.....	56
7.5.2 Fournitures de l'administration.....	56
7.5.3 Livrables de la prestation.....	56
7.5.4 Compétences recherchées.....	56
7.5.5 Niveau de complexité et délai de réalisation minimum.....	56
8 Présentation des unités d'œuvre (UO) du lot 3.....	57
8.1 UO ISP - Intégration de la Sécurité dans les Projets.....	57
8.1.1 Contenu de la prestation.....	57
8.1.2 Fournitures de l'administration.....	58
8.1.3 Livrables de la prestation.....	58
8.1.4 Compétences recherchées.....	59
8.1.5 Niveau de complexité et délai de réalisation minimum.....	59
8.2 UO SGP - étude de sensibilité globale du projet.....	60
8.2.1 Contenu de la prestation.....	60
8.2.2 Fournitures de l'administration.....	60
8.2.3 Livrables de la prestation.....	60
8.2.4 Compétences recherchées.....	61
8.3 Niveau de complexité et délai de réalisation minimum.....	61
8.4 UO EVP - Étude d'impact sur la vie privée.....	61
8.4.1 Contenu de la prestation.....	61
8.4.2 Fournitures de l'administration.....	62
8.4.3 Livrables de la prestation.....	62
8.4.4 Compétences recherchées.....	62
8.4.5 Niveau de complexité et délai de réalisation minimum.....	63
8.5 UO CDS - Contrôle Développement et audits Sécurité.....	64
8.5.1 Contenu de la prestation.....	64
8.5.2 Fournitures de l'administration.....	66
8.5.3 Livrables de la prestation.....	66
8.5.4 Compétences recherchées.....	67
8.5.5 Niveau de complexité et délai de réalisation minimum.....	67
8.6 UO ESA – Étude de sécurité applicative.....	68
8.6.1 Contenu de la prestation.....	68
8.6.2 Fournitures de l'administration.....	68
8.6.3 Livrables de la prestation.....	68
8.6.4 Compétences recherchées.....	69
8.6.5 Niveau de complexité et délai de réalisation minimum	69
9 Présentation des unités d'œuvre (UO) du lot 4.....	69
9.1 GR – Gestion des risques informatiques.....	69
9.1.1 Contenu de la prestation.....	69
9.1.2 Fournitures de l'administration.....	71
9.1.3 Livrables de la prestation.....	71
Les livrables principaux attendus pour la prestation sont :.....	71
9.1.4 Liste des outils existants.....	72
9.1.5 Niveau de complexité et durée de réalisation.....	72
9.2 OF – Outils de formation.....	73

9.2.1	Contenu de la prestation.....	73
9.2.2	Fournitures de l'administration.....	74
9.2.3	Livrables de la prestation.....	75
	Les livrables principaux attendus pour la prestation sont :.....	75
9.2.4	Liste des outils existants.....	75
9.2.5	Niveau de complexité et délai de réalisation minimum.....	75
9.3	OS – Outils de sécurité.....	76
9.3.1	Contenu de la prestation.....	76
9.3.2	Fournitures de l'administration.....	78
9.3.3	Livrables de la prestation.....	78
	Les livrables principaux attendus pour la prestation sont :.....	78
9.3.4	Liste des outils existants.....	78
9.3.5	Niveau de complexité et délai de réalisation minimum.....	79
9.4	Formations à la sécurité informatique.....	80
10	Annexes.....	81
10.1	Périmètre des missions et organisation de la Direction générale des Finances publiques..	81
10.2	Cadre d'architecture et exemple d'études.....	81
10.3	Modèles.....	82
10.4	Cadre pour le développement.....	82
10.5	Accessibilité et ergonomie.....	82
10.6	Conditions de sécurité.....	83

1 Présentation générale de la consultation

1.1 **Objet du marché**

Le présent appel d'offres a pour objet un ensemble de prestations intellectuelles informatiques relatives au système d'information de la DGFIP¹. Les prestations couvrent les besoins en urbanisation du SI relevant de la DTNUM², décrites dans le lot 1, la mise en œuvre des comités d'architecture informatique et les prestations qui en découlent relevant du bureau SI1, décrites dans le lot 2, la sécurité des applications et les prestations qui en découlent relevant également du bureau SI1, décrites dans le lot 3, et les besoins en outils de sécurité, décrits dans le lot 4, dans le périmètre fonctionnel du même bureau.

Le marché doit notamment permettre la réalisation d'études d'urbanisation et d'analyses de processus ciblés, la réalisation de prestations d'assistance dans le cadre des travaux réguliers d'instructions de dossiers d'architecture applicative, d'études d'architecture applicative et/ou fonctionnelle, d'audits, de constitution de cadres normatifs et de sécurité du système d'information de la DGFIP. Ce contexte est matérialisé entre autres par son cadre d'architecture³, dont l'évolution et la mise en œuvre opérationnelle nécessitent des prestations d'assistance et de mise à jour de documents techniques de la DGFIP.

L'appel d'offres doit permettre également la fourniture de prestations d'analyse de risques, s'appuyant sur une méthodologie dérivée d'EBIOS 2010 et d'ISO 27k. Les livrables attendus du titulaire alimenteront le dossier de sécurité dans le cadre des homologations de sécurité des applications de la DGFIP.

Les prestations objet de l'appel d'offre doivent aussi permettre de réaliser des contrôles de code sur la sécurité applicative. Les audits de sécurité du code ont pour objet d'évaluer le respect des bonnes pratiques de sécurité, d'identifier de possibles failles de sécurité dans le code des applications et de proposer au projet un plan d'actions pour la correction des anomalies détectées en matière de sécurité.

Les prestations objets de l'appel d'offres doivent permettre à la DGFIP de rationaliser son système d'information et de répondre aux besoins d'études, de conseils et d'expertises en matière d'architecture applicative et/ou fonctionnelle dans l'environnement des nouvelles technologies, appliquées au contexte de la DGFIP.

1.2 **Allotissement**

La consultation est allotie de la façon suivante :

- **Lot 1** : Réalisation d'études d'urbanisation ou d'analyses ciblées de processus fonctionnel ou métier ;

1 Direction Générale des Finances Publiques

2 Délégation à la Transition Numérique de la DGFIP

3 Le cadre d'architecture est disponible en annexe de ce CCTP

- **Lot 2** : Réalisation d'instructions de dossiers d'architecture et d'études d'architecture fonctionnelle et/ou applicative sur des environnements classiques ou Cloud privé. Mises à jour des documents du cadre d'architecture ;
- **Lot 3** : Réalisation d'analyses de risques d'applications et d'audits de sécurité, études de sécurité applicative ;
- **Lot 4** : Veille relative aux outils sécurité et prestations annexes.

1.3 Présentation de la DGFIP

La DGFIP est une des directions du Ministère de l'Économie, des Finances et de la Souveraineté industrielle, énergétique et numérique

La DGFIP exerce une grande variété de missions :

- des missions fiscales : la gestion des contribuables, la détermination des bases d'imposition et le calcul des impôts, le recouvrement des impôts, le contrôle fiscal des déclarations déposées et la recherche des contribuables défaillants ;
- des missions foncières : la tenue du cadastre, le contrôle des opérations immobilières des collectivités publiques, la publicité foncière ;
- des missions d'expertise et de contrôle : le contrôle financier, la mission d'expertise économique et financière ;
- des missions comptables : la gestion financière des comptes de l'État, du secteur public local et hospitalier (recettes, dépenses, comptabilité).

1.4 Structures de la DGFIP

Pour assurer ses missions, la DGFIP s'appuie sur :

- une **administration centrale** qui exerce des fonctions de pilotage, de coordination, d'animation, d'expertise et de soutien pour l'ensemble des structures de la DGFIP. Les services centraux sont structurés en services, sous-directions et bureaux ;
- des **services territoriaux** répartis sur tout le territoire national. Ces services ont une compétence nationale et/ou spéciale, régionale ou départementale ;
- des **services locaux**.

La DGFIP s'appuie également sur la **Délégation à la Transformation Numérique**, ou DTNum, créée le 1^{er} janvier 2021 par [l'arrêté du 20 décembre 2019 portant organisation de la direction générale des finances publiques](#).

Rattachée au directeur général, la DTNum a été **réorganisée en septembre 2024 en 5 pôles** et une mission pour répondre à son nouvel objectif : **construire une organisation apprenante et sobre, centrée sur l'utilisateur et pilotée par la donnée**.

Parmi les services centraux, le **SSI**⁴ assure le pilotage des missions de l'informatique et définit les orientations et les stratégies pour la DGFIP en matière informatique. Au sein de

4 Service des Systèmes d'Information

cette structure, le bureau de l'architecture et des normes (SI1) est chargé :

- d'alimenter et d'animer la réflexion stratégique ;
- de décliner la stratégie au travers de méthodes, de règles ;
- d'accompagner les bureaux de MOE⁵ et MOA⁶ dans leur mise en œuvre par les projets ;
- d'auditer et recenser les pratiques et de contrôler le respect des principes par les projets. **Le bureau de l'architecture et des normes (SI1), division DAN, équipes Architecture Applicative et Sécurité du Système d'Information seront les principaux utilisateurs du présent marché.**

Les autres services de la structure SSI sont :

- le **DRS** (Département des Ressources et du support) : gère les fonctions RH, budget, marché et la protection des données pour l'ensemble du réseau informatique, anime la gouvernance du SSI en matière de planification d'activité et d'attribution des missions ;
- le **bureau du pilotage de la production et du service aux utilisateurs** (SI2) : en charge du pilotage de l'exploitation, de l'assistance, de l'éditique et de la téléphonie ;
- le **bureau des infrastructures et de la sécurité** (SI3) : porte les infrastructures informatiques mutualisées de la DGFiP (data centers, réseau, serveurs mutualisés, infrastructures de données, de sauvegarde, de sécurité, de supervision, les postes de travail) et le centre opérationnel de sécurité de la DGFiP (SOC).

Parmi les autres acteurs de la structure SSI figure également la Direction des Projets Numériques (DPN) qui regroupe 17 structures en charge des activités de MOE et MOA :

- la **mission SIRHIUS** : pilote le système d'information RH interministériel Sirhius dans tous ses aspects de MOA transverse, MOA DGFiP et MOE transverse ;
- la **direction des projets RH** (DP1) : pilote les projets de la sphère RH en rassemblant les équipes MOA et MOE associées ;
- la **direction de projet PILAT**⁷ (DP2) : pilotage unifié MOA et MOE du projet PILAT ;
- la **direction de projet ROCSP**⁸ (DP3) : pilotage unifié MOA et MOE du projet RocSP ;
- la **direction des projets des particuliers** (DP4) : pilote les projets de la sphère des particuliers ;
- la **direction de projet E-Enregistrement**⁹ (DP5) : pilotage unifié MOA et MOE du projet E-Enregistrement ;

5 MOE : Maîtrise d'œuvre informatique

6 MOA : Maîtrise d'ouvrage informatique

7 Bascule pour la refonte du SI du contrôle fiscal

8 Extension de l'application RSP pour le recouvrement forcé

9 Dématérialisation de l'enregistrement des dons manuels, des successions, des cessions de droits sociaux, ...

- la **direction de projet des référentiels** (DP6) : pilotage unifié MOA et MOE des référentiels de la DGFIP ;
- la **direction de projet des services aux usagers** (DP7) : pilotage unifié MOA et MOE des services offerts aux usagers ;
- la **direction de projet des professionnels** (DP8) : pilote les projets de la sphère des professionnels ;
- la **Direction de Projet des échanges internationaux de données** (DP9) : a pour mission de regrouper la mise en œuvre informatique des conventions internationales fiscales signées par la France, au niveau de l'OCDE et de l'UE ;
- le **bureau de l'environnement de travail et des applications des agents** (BSI1) : pilote le développement des outils quotidiens transverses des agents : messagerie, visioconférence, mobilité, portail Ulysse, portail agent, PIGP¹⁰, annuaire agents (volet MOA), Nausicaa¹¹, ITM¹², applications RH en production (hors Sirhius) ;
- le **bureau des applications du foncier, du patrimonial, de la sécurité juridique et du contrôle fiscal** (BSI2) : pilote le développement des applications en production de ces domaines ;
- le **bureau des applications des professionnels** (BSI3) : pilote le développement des applications en production de ce domaine ;
- le **bureau des applications des particuliers** (BSI4) : pilote le développement des applications en production de ce domaine et les projets de modernisation de la taxation, du recouvrement et du recoupement ;
- le **bureau des applications du secteur public local** (BSI5) : pilote le développement des applications en production de ce domaine ;
- le **bureau des applications de la comptabilité, de la dépense de l'État et du domaine** (BSI6) : pilote le développement des applications en production de ce domaine ;
- le **bureau de l'intégration** (BINT) : contribue de façon majeure à la fabrication des projets ou des maintenances dans les étapes d'intégration inter-applicative, d'architecture technique et d'intégration de l'exploitabilité.

10 Portail Internet de la Gestion Publique <https://portail.dgfip.finances.gouv.fr/portail/accueilIAM.pl>

11 Gestion et publication de la documentation officielle de la DGFIP sur l'intranet

12 Interface de restitution des traces métiers créées par les applications

1.5 Le SI DGFIP en 2025

1.5.1 Des agents au cœur du système d'information

Avec plus de 5 000 agents exerçant directement leurs missions dans les services informatiques, la DGFIP représente plus du quart des effectifs de l'informatique civile de l'État. La combinaison équilibrée de ces moyens, internes et externes, a permis de lancer de nombreux projets innovants, tout en étant vigilant sur le niveau de maîtrise interne de l'environnement technique et fonctionnel du système d'information.

1.5.2 Une organisation qui a évolué

Pour répondre aux besoins croissants et légitimes de l'ensemble de ses utilisateurs, qu'ils soient usagers, partenaires ou agents, et pour accompagner les métiers dans les transformations qu'ils portent, la DGFIP adapte régulièrement ses services numériques.

1.5.3 Des projets au service du système d'information

Le SSI pilote, développe et maintient près de 800 applications ou produits (785 recensés en décembre 2024), en interaction les unes avec les autres, qui soutiennent les politiques publiques confiées à la DGFIP ou à la communauté interministérielle, que ce soit lors d'événements exceptionnels ou de dispositifs installés dans la durée.

Une action de modernisation est engagée dans la durée pour résorber la dette technologique, sur l'ensemble des composantes applicatives qui constituent le cœur de gestion des missions. Elle doit permettre de réduire les budgets d'achat propriétaire et d'harmoniser les architectures pour mobiliser de manière plus souple les ressources.

1.5.4 Des technologies et une méthode

En termes de technologies, l'orientation par défaut vers le cloud privilégiant les cycles courts, les méthodes de construction itératives et favorisant l'amélioration des phases de tests, tout en restant à l'état de l'art, entraîne des évolutions en termes de méthode.

1.6 Les grands principes directeurs du SI de la DGFIP

L'identification des principes de fabrication numériques de la DGFIP repose sur une triple approche :

- capitaliser sur l'expérience acquise et expliquer les valeurs portées par la DGFIP ;
- tirer les enseignements des réflexions menées, en interne et en externe, face aux difficultés rencontrées ;
- se préparer aux défis opérationnels à venir.

Elle vise à expliciter des principes d'action, déclinés en pratiques structurantes qui portent la conception, le déploiement et l'évolution des solutions numériques.

Les principes directeurs structurants sont listés ci-dessous :

- **Mettre l'utilisateur au centre** : la DGFIP positionne l'utilisateur au centre de son activité. Il s'agit de l'inscrire en tant qu'acteur clef du système d'information, plutôt que comme son consommateur ;
- **Développer l'accessibilité** : la DGFIP s'inscrit pleinement dans le RGAA. La démarche de mise en conformité s'étend sur toutes les étapes de conception et de réalisation ;
- **Avoir une attention constante à la disponibilité** : la disponibilité désigne la capacité du système à être opérationnel et accessible aux utilisateurs, en minimisant le nombre ainsi que la durée des interruptions et des pannes. Il est attendu des produits numériques qu'ils soient disponibles à tout moment car il s'agit d'outils indissociables de l'activité des agents de la DGFIP et des services offerts aux usagers et aux partenaires ;
- **Porter la politique écoresponsable** : la DGFIP s'engage résolument pour apporter sa contribution dans la lutte contre les émissions de gaz à effet de serre (GES). Une acculturation à l'écoconception numérique (formation et projet) est fortement recherchée, notamment en intégrant le Référentiel général d'écoconception de services numériques (RGESN) dans le cycle de conception des produits;
- **S'appuyer sur une démarche constante de réduction de la dette technique** : la DGFIP maintient une démarche de mise en conformité technologique, afin de réduire les risques d'obsolescence technique ou contractuelle, qui pourraient conduire à des investissements contraints ou à des réductions de niveau de service ;
- **S'orienter vers le cloud** : la DGFIP oriente par défaut les projets sur le Cloud en accord avec la directive interministérielle « Cloud au centre ». L'enjeu pour la DGFIP est de mieux automatiser la gestion des opérations techniques, réduire les coûts et les délais de livraison, contribuer à la mise en conformité technologique, faciliter la prise en compte de la résilience et maintenir son attractivité dans ses recrutements ;
- **Déployer l'intelligence artificielle (IA)** : la DGFIP a pour ambition de développer une IA souveraine, conforme et frugale. Ces ambitions se traduisent par la mise en place d'une plateforme de rationalisation des outils d'Intelligence Artificielle, un accompagnement à l'expérimentation et l'industrialisation des projets métier sur le volet IA, ainsi que la réalisation d'une veille technologique continue grâce à un environnement de travail à l'état de l'art.
- **Déployer le DevOps** : le DevOps est le mode d'organisation retenu pour les applications rejoignant le cloud ;
- **Favoriser l'utilisation des méthodes agiles** : la construction et la maintenance du système d'information de la DGFIP s'appuient massivement sur la méthodologie « Cycle en V ». Les méthodes agiles sont utilisées quand elles sont possibles et utiles notamment pour les nouveaux projets sur le Cloud privé NUBO ;

- **Fiabiliser et valoriser les données** : la DGFIP acquiert, produit et valorise des données au bénéfice de ses missions. Elle favorise la réutilisation en interne des données par des API et commence à ouvrir davantage ses données en externe ;
- **Être attentif à la dépendance aux fournisseurs et à la souveraineté** : Le SSI pilote sa dépendance aux fournisseurs de services, de matériels et de logiciels.

1.7 Pilotage global du marché

L'administration organisera les deux instances de suivi du marché qui assurent les différentes relations entre le titulaire et l'administration : le comité de pilotage (COPIL) et le comité de suivi (COSUI).

1.7.1 Le comité de pilotage

Le comité de pilotage (COPIL) a pour objectif de s'assurer du respect des obligations prises par le titulaire et l'administration dans le cadre du marché. D'une fréquence trimestrielle, il est présidé pour le lot 1 par le chef de pôle UX de la DTNum ainsi que par le responsable Urbanisation du SI qui pilote le marché pour le compte de la DTNum. Pour les lots 2, 3 et 4, il est présidé par le chef du bureau de l'architecture et des normes qui pilote ce marché pour le compte du bureau SI1. Pour chacun des lots, il regroupe des responsables du titulaire, dont au moins le directeur de projet en charge des aspects opérationnels de ce marché.

La date et l'ordre du jour seront arrêtés par l'administration.

Le titulaire du marché rédigera :

- Les documents entrants qui devront être soumis pour approbation à la DTNum et au bureau de l'architecture et des normes (SI1) au plus tard deux semaines avant chaque COPIL, mentionnant a minima :
 - le bilan des actions réalisées, suivi de celles en cours et propositions éventuelles ;
 - le suivi des commandes ;
 - le suivi des niveaux de services : requis et obtenus ;
 - Suivi des pénalités appliquées pour non respect des engagements ;
 - le suivi des points soulevés en COSUI (actions, décisions, risques) ayant des impacts en termes contractuels ou de qualité de service.
- Les comptes-rendus qui devront être soumis pour approbation à la DTNum et au bureau de l'architecture et des normes (SI1) au plus tard une semaine après chaque COPIL. Le bureau de l'architecture et des normes (SI1) validera ces comptes-rendus et en assurera la diffusion au sein de la DGFIP.

1.7.2 Le comité de suivi

Le comité de suivi (COSUI) a pour objectif d'assurer le suivi régulier des activités du prestataire pour chaque bureau ayant commandé des UO. Il permet d'échanger sur la

qualité de service et de décider des actions de remise en conformité si nécessaire. Il permet également de traiter les problèmes courants (humains, organisationnels, matériels).

D'une fréquence mensuelle, il regroupe le directeur de projet en charge des aspects opérationnels de ce marché ainsi que, pour l'administration, le responsable ayant commandé les UO.

La date et l'ordre du jour seront arrêtés par l'administration.

Pour chaque COSUI, le titulaire adressera à l'administration l'ensemble des documents supports une semaine avant le COSUI, et en particulier les documents justifiant des prestations réalisées.

Le compte-rendu sera soumis par le titulaire pour approbation au plus tard une semaine après le COSUI.

Après validation par le bureau ayant commandé les UO, ce compte-rendu sera transmis par le titulaire à la DTNum et au bureau de l'architecture et des normes (SI1) pour être versé aux documents entrants du COPIL suivant.

1.8 Description des unités d'œuvre (UO)

Les unités d'œuvre sont définies par :

- le contenu de la prestation ;
- les fournitures de l'administration ;
- les livrables de la prestation ;
- les compétences recherchées ;
- le niveau de complexité avec délai de réalisation minimum de réalisation en jours.

Tous les contacts, directs ou téléphoniques, ainsi que toutes les correspondances et les documentations devront être réalisés en français exclusivement.

Tous les livrables mentionnés devront être fournis sous forme papier et dématérialisée sous forme de fichier au format OpenDocument ou lisibles avec LibreOffice a minima sans modification de la mise en page, et compatible avec la version du logiciel utilisé par l'administration.

1.9 Exigences communes aux trois lots

- Les prestations seront effectuées sur les sites de l'administration en Île-de-France, à Fontenay sous bois (94) pour le lot 1 et essentiellement à Noisy-le-Grand (93) ; pour le lot 3 une partie pourra être réalisée depuis l'ESI de Rennes. Les exigences sur les équipements des intervenants ainsi que sur le travail distant et le télétravail sont précisées dans les annexes de ce CCTP ; Pour le lot 4, les prestations seront effectuées soit sur le site de Noisy le Grand, soit à distance sous réserve

d'autorisation expresse pour certaines prestations.

- Dans le cas où le prestataire serait autorisé à effectuer sa mission ou une partie de sa mission en télétravail, il devra disposer d'un accès téléphonique permettant le transfert d'appel (aucun téléphone portable ni ligne téléphonique ne sera fourni par l'administration) ;
- Le titulaire indiquera le contenu des actions de formation et de sensibilisation aux enjeux de sécurité et de confidentialité qu'il a entrepris auprès des personnels amenés à intervenir dans le cadre de ce marché ;
- Le titulaire devra fournir préalablement à la prestation le curriculum vitae des personnes qu'il présentera à l'administration pour réaliser la prestation. La DGFiP se réserve le droit de récuser à tout moment toute personne qui ne posséderait pas les compétences requises ;
- Dans le cas du recours à la sous-traitance, le titulaire devra présenter son sous-traitant pour agrément par l'administration conformément aux dispositions du CCAP ;
- Les prestations donnent lieu à la remise de livrables finaux. Certaines UO comportent des livrables intermédiaires. Tous les livrables réalisés sont la propriété de la DGFiP ;
- Les délais de remise des livrables intermédiaires sont d'un mois, sauf mention contraire précisée dans le descriptif de l'UO ;
- Les délais de remise des livrables finaux correspondent aux délais de réalisation de chaque UO ;
- Le délai de validation des livrables intermédiaires et finaux est d'un mois (décompté de quantième à quantième) sauf mention contraire précisée dans le descriptif de l'UO ;
- Le titulaire devra respecter les méthodologies mises en œuvre au niveau du système d'information de la DGFiP ;
- Le titulaire devra respecter les annexes du présent document ;
- Les délais exprimés en jours correspondent à des jours ouvrés ;
- Les délais exprimés en mois sont décomptés de quantième à quantième ;
- **Les UO incluent les charges de pilotage, de reporting et de coordination de la prestation**, et en particulier la tenue des instances de pilotage du marché prévue au chapitre [#1.7.Pilotage global du marché|outline](#) du présent CCTP. Le titulaire devra prévoir et préciser les actions mises en œuvre pour s'assurer d'une veille technique de ses équipes ;
- Sauf indications contraires dans la description de l'UO, un projet s'entend comme un ensemble fonctionnel cohérent (il peut s'agir en réalité d'un projet ou d'un sous-projet) ou une partie du système d'information de l'administration (ensemble de

processus transversaux de traitements de l'information qu'il soit en phase d'étude ou en exploitation) ;

- Les délais de réalisation minimum en jours indiqués dans les tableaux descriptifs des UO sont contractuels. Ce sont des délais retenus par l'administration pour la réalisation de chaque unité d'œuvre par un seul profil, en fonction des retours d'expérience et des attentes en termes de qualité des prestations ;
- Les comptes rendus de réunion décrits dans les UO ci-dessous doivent être fournis à l'administration dans un délai d'une semaine maximum après le déroulement de la réunion à laquelle ils se rapportent, sauf mention contraire précisée dans le descriptif de l'UO ;
- Les supports de présentation de réunion des instances de gouvernance qui constituent des livrables dans les UO décrites ci-dessous doivent être fournis à l'administration dans un délai d'une semaine minimum avant le déroulement de la réunion à laquelle ils se rapportent, sauf mention contraire précisée dans le descriptif de l'UO.
- L'utilisation de l'Intelligence Artificielle est par principe proscrite pour la réalisation des prestations du marché. Elle ne pourra être mise en œuvre par le titulaire qu'avec l'accord explicite et écrit de l'administration.

1.10 Exigences qualité associées aux prestations

1.10.1 Garantie de qualifications minimales et de stabilité pour les intervenants

Le titulaire a l'obligation de fournir des profils conformes à son offre technique et au CCTP pour atteindre les objectifs fixés. Ces équipes ont l'expérience des projets de réalisation ayant des environnements organisationnel, fonctionnel et technologique les plus proches possibles de ceux couverts par le marché.

Dans ce cadre, des profils types à respecter a minima par le titulaire tout au long de l'exécution du marché sont définis par l'administration. Les tableaux des profils minima pour les intervenants principaux sont détaillés ci-dessous.

Lot 1	Nombre minimal d'années d'expérience		
	Expérience professionnelle en informatique	Expérience professionnelle en architecture d'entreprise et urbanisation fonctionnelle	Expérience professionnelle en maîtrise d'ouvrage ou maîtrise d'œuvre
Profils types (niveau de diplôme)			
Urbaniste expert (bac +5 ou équivalent)	10 après le diplôme	5 ans	5 ans

Lot 1	Nombre minimal d'années d'expérience		
	Expérience professionnelle en informatique	Expérience professionnelle en architecture d'entreprise et urbanisation fonctionnelle	Expérience professionnelle en maîtrise d'ouvrage ou maîtrise d'œuvre
Urbaniste intermédiaire (bac +5 ou équivalent)	5 après le diplôme	2 ans	3 ans
Urbaniste junior (bac +5 ou équivalent)	1 après le diplôme (si ancien apprenti) 2 ans sinon		2 ans minimum

Dans ce tableau, chaque profil est caractérisé par une expérience minimale en nombre d'années dans l'informatique, un diplôme type et une expérience minimale sur une ou plusieurs des expertises nécessaires et adaptées au contexte du projet :

Urbaniste expert :

- Diplôme requis par ordre de priorité bac +5 et grandes écoles :
 - 1 : Diplôme d'une grande école d'ingénieur (exemple : Mines de Paris, Télécom Paris, L'Efrei, EPITA EPITEC...)
 - 2: Master 2 MIAGE (Méthodes Informatiques Appliquées à la Gestion des Entreprises)
 - 3 : Master 2 Management des systèmes d'information ou équivalent et ou grande école de commerce parcours technologie du numérique (exemple : ESSEC Business School, EM Lyon...)
- Expérience professionnelle : l'urbaniste expert est une personne qui dispose d'une solide expérience en matière de cartographie, d'architecture fonctionnelle, de maîtrise d'ouvrage et d'urbanisation. Cette personne a également travaillé au sein d'une ou plusieurs administrations publiques et est familiarisée avec l'environnement administratif français. Enfin, elle est capable d'analyser rapidement les problématiques SI, ainsi qu'un nombre d'informations important, de les synthétiser et de les présenter de manière simple et pédagogique. Elle maîtrise la modélisation de processus quel que soit leur niveau de complexité. Elle s'adapte et apprend rapidement à se servir des outils utilisés par l'équipe urbanisation (outil YED ou équivalent).

Urbaniste intermédiaire :

- Diplôme requis par ordre de priorité bac +5 et grandes écoles :
 - 1 : Diplôme d'une grande école d'ingénieur (exemple : Mines de Paris, Télécom Paris, L'Efrei, EPITA EPITEC...)

- 2: Master 2 MIAGE (Méthodes Informatiques Appliquées à la Gestion des Entreprises)
- 3 : Master 2 Management des systèmes d'information ou équivalent et ou grande école de commerce parcours technologie du numérique (exemple : ESSEC Business School, EM Lyon...)
- Expérience professionnelle : l'urbaniste intermédiaire dispose d'une expérience solide en architecture fonctionnelle, MOA et urbanisation. Il a au moins une à deux expériences professionnelles au sein d'une administration publique ou d'entités privées ayant un SI comparable à la DGFIP. Il sait analyser les problématiques récurrentes rencontrées au sein d'un grand SI, les présenter de manière simple et pédagogique. Il maîtrise la modélisation de processus quel que soit leur niveau de complexité. Il s'adapte et apprend rapidement à se servir des outils utilisés par l'équipe urbanisation (outil YED ou équivalent).

Urbaniste junior :

- Diplôme requis par ordre de priorité bac +5 et grandes écoles :
 - 1 : Diplôme d'une grande école d'ingénieur (exemple : Mines de Paris, Télécom Paris, L'Efrei, EPITA EPITEC...)
 - 2: Master 2 MIAGE (Méthodes Informatiques Appliquées à la Gestion des Entreprises)
 - 3 : Master 2 Management des systèmes d'information ou équivalent et ou grande école de commerce parcours technologie du numérique (exemple : ESSEC Business School, EM Lyon...)
- Expérience professionnelle : l'urbaniste junior dispose d'une expérience en architecture fonctionnelle, MOA et urbanisation. Il a une expérience professionnelle passée dans le secteur public et ou privé. Il maîtrise la modélisation de processus et a les aptitudes pour être fonction-support au sein de l'équipe.

Connaissances de base pour l'ensemble des profils sur les notions suivantes : Java Full-Stack, API SOAP, API REST, SQL et des connaissances en modèle de données (MPD, MCD...). Big Data / Data Mining, Open Data, architecture Cloud et architecture des échanges de données synchrones et asynchrones. Enfin les candidats disposeront de connaissances en matière de droit informatique et liberté et de RGPD.

Lot 2	Nombre minimal d'années d'expérience		
Profils types (niveau de diplôme)	Expérience professionnelle en informatique	Expérience technologique dans le domaine des nouvelles technologies	Expérience professionnelle en architecture
Architecte fonctionnel expert (bac + 5 ou équivalent)	7 ans après le diplôme	4 ans minimum	4 ans minimum* (* expérience en architecture fonctionnelle, urbanisation, AMOA, analyste métier obligatoire)
Architecte applicatif expert (bac +5 ou équivalent)	9 ans après le diplôme	5 ans minimum	5 ans minimum** (** expérience en architecture applicative et technique obligatoire)
Architecte Cloud expert (bac + 5 ou équivalent)	7 ans après le diplôme	4 ans minimum	4 ans minimum *** (*** expérience en architecture Cloud privé, open stack recommandé)

Lot 3	Nombre minimal d'années d'expérience		
Profils types (niveau de diplôme))	Expérience professionnelle en informatique et diplôme type	Expérience technologique dans le domaine des nouvelles technologies	Expérience professionnelle en sécurité
Expert en risques numériques (bac + 4 ou équivalent)	9 ans d'expérience dans des SI de sensibilité et de complexité similaires à celui de la DGFIP (après le diplôme))	6 ans	3 ans
Consultant en sécurité des SI (bac + 4 ou équivalent)	4 années après le diplôme	3 ans	2 ans
Expert en sécurité applicative (bac + 4 ou équivalent)	9 ans d'expérience dans des SI de sensibilité et de complexité similaires à celui de la DGFIP (après le diplôme)	6 ans	3 ans
Auditeur de sécurité du code (bac + 4 ou équivalent)	4 années après le diplôme	3 ans	2 ans

Dans ces tableaux, chaque profil est caractérisé par une expérience minimale en nombre d'années dans l'informatique, un diplôme type et une expérience minimale sur une ou plusieurs des expertises nécessaires et adaptées au contexte du projet :

- Technologique, dans les orientations de la DGFIP : Java J2EE, Java, SOAP, REST, DRUPAL et PHP. Des profils d'experts sont demandés dans les thématiques IA (Intelligence Artificielle), bases de données avancées (optimisation, réplication...), décisionnel, Big Data / Data Mining, Open Data, architecture du Cloud privé et architecture des échanges de données synchrones et asynchrones (notamment recouvrant la notion d'APIM et en lien avec les nouveaux protocoles d'échanges OIDC, norme eIDAS) ;
- Professionnelle, en architecture fonctionnelle, en architecture applicative, en architecture des échanges sur les architectures cibles citées dans le cadre d'architecture de la DGFIP mais aussi sur la prise en main d'un écosystème du Cloud privé et des connaissances sur l'impact juridique du RGPD sur les architectures applicatives cloisonnées par zone d'usage (pour le lot 2) ou en sécurité (pour le lot 3).

L'architecte fonctionnel expert est le garant de la cohérence fonctionnelle d'un projet au sein d'un système d'information. Il doit construire une architecture fonctionnelle cible dans le respect des principes et standards présents dans le cadre d'architecture. L'architecture fonctionnelle est le premier jalon en amont de la conception de l'architecture applicative et au plus proche du projet, de la notion de données et du concept d'objet racine. Garant de la cohérence du système, il évalue la pertinence et la cohérence des projets par rapport à cette architecture cible et aux systèmes existants. Son expertise lui permet de conseiller efficacement le projet en phase d'expression de besoin. Il maîtrise les techniques de coordination de projet. Les profils présentés devront montrer une expérience dans des SI de sensibilité et de complexité similaires à celui de la DGFIP, s'orientant vers les API. La mise en œuvre d'une démarche DDD¹³ sera un plus.

L'architecte applicatif expert est le garant de la cohérence de l'architecture des différentes applications sur les principes fondamentaux élaborés dans le cadre d'architecture de la DGFIP. Pour proposer des modèles dans le cadre de la définition de l'architecture de référence, il collabore avec les différents architectes (et notamment avec les architectes projet en charge de présenter une architecture applicative que l'architecte applicatif expert devra analyser). Il est en capacité de concevoir l'architecture des nouvelles applications du système d'information couvrant les couches N-tiers (présentation, données, traitement) en accompagnant les équipes projet en support et

¹³ DDD (Domain-Driven Design ou Conception pilotée par le domaine) est une pratique de conception popularisée à partir de 2003 par Éric Evans, qui repose sur 2 aspects :

- un langage dit ubiquitaire, structuré autour du modèle du domaine et utilisé par tous les membres de l'équipe, aussi bien par les profils techniques que métiers ;
- un modèle utilisant ce langage, et étant une abstraction qui décrit les concepts sélectionnés d'un domaine métier ainsi délimité, ainsi que leurs relations.

conseil. L'architecte applicatif doit savoir assembler et configurer conceptuellement les composants matériels ou logiciels dans le respect des standards techniques et des règles de sécurité du SI. Par ses connaissances, il participe à l'élaboration de normes de conception technique. Les profils proposés pour les revues d'architecture devront faire preuve d'autonomie, de nombreux acteurs étant impliqués. Ils devront par ailleurs bien connaître le contexte de la DGFIP et son cadre d'architecture (cet appel d'offres contient une UO de prise de connaissance de ce contexte ainsi que du cadre d'architecture qui pourra être utilisée par la DGFIP pour les premiers intervenants).

L'**architecte Cloud expert** est un expert confirmé dans le domaine des architectures au sein de Cloud privé. En capacité d'effectuer des prototypes, il doit pouvoir répondre aux différentes problématiques pour mettre en œuvre un nouveau cadre normatif cohérent et commun pour les applications sur le Cloud privé de la DGFIP allant de la définition d'une plateforme d'intégration et de livraison continues (chaîne de CI/CD) au cloisonnement réseau. Des connaissances sont attendues dans la virtualisation (OpenStack, SWIFT, ANSIBLE), conteneurs (Kubernetes, Docker) gestion des secrets (Vault, Keycloak), la gestion des données (Restic), la gestion de l'observabilité (Loki, Prometheus, Grafana), la gestion des logs (ELK, Graylog) et de manière générale sur la connaissance des architectures et logiciels sur des plateformes Cloud privé IaaS et PaaS.

Les profils d'**expert en risques numériques** et **consultant en sécurité des SI** sont demandés pour les UO ISP et EVP. Ils nécessitent des connaissances approfondies sur la sécurité, ainsi que sur la maîtrise des risques. Une très bonne connaissance de la réglementation relative à la sécurité et à la protection des données est également attendue (notamment RGS V2, EBIOS, NIS V2, RGPD).

Les profils d'**expert en sécurité** des SI et **auditeurs de sécurité du code** sont les garants de la sécurisation du SI de la DGFIP. Des compétences avancées sont attendues en Java et PHP ainsi qu'en sécurité applicative et en tests d'intrusion.

Conformément à son obligation de résultat, le titulaire est responsable de la formation et de la mise à niveau des compétences indispensables pour son personnel sur l'ensemble des sujets relevant des prestations demandées. Il en assume l'incidence sur l'organisation de la prestation et prend en charge l'intégralité des coûts associés.

Le titulaire devra prévoir la mise à niveau (éventuellement l'outillage le permettant) pour permettre l'échange et le partage mutualisés des connaissances techniques et normatives de la DGFIP auprès de l'ensemble du personnel au sein d'une même unité de travail (pour assurer la même qualité de service de l'ensemble de son personnel au sein de la même unité de travail).

Par ailleurs, l'équipe mise en place tout au long de l'exécution du marché doit satisfaire à des exigences de stabilité et de recouvrement en cas de remplacement qui sont fixées par le CCAP.

Le remplacement d'un intervenant ne doit en aucun cas impacter le niveau de qualité et de service, ni entraîner de délai ou de coût supplémentaire(s) pour l'administration. Ainsi, tout remplacement d'un intervenant induit :

- une formation du nouvel intervenant au contexte spécifique de la DGFiP, équivalente à celle délivrée par l'UO PRC, mais à la charge du titulaire ;
- une période de recouvrement d'au moins 20 jours ouvrés consécutifs et à temps plein entre les deux intervenants pris en charge par le titulaire, sauf cas de force majeure dûment justifié.

1.10.2 Niveaux de service et pénalités

En fonction des décisions prises par l'administration à l'issue des vérifications et au cours des prestations, des pénalités peuvent être déclenchées en application des dispositions du CCAP.

Le présent paragraphe précise les niveaux de service attendus ainsi que les pénalités prévues dans le CCAP en cas de défaut de qualité de service.

Trois indicateurs sont prévus pour mesurer le niveau de service :

- la stabilité des équipes : afin d'assurer une continuité dans les expertises apportées, tous postes confondus ;
- la qualité des intervenants proposés : les intervenants doivent correspondre aux profils exigés dans le CCTP, aux compétences attendues précisées dans les UO et proposés par le titulaire dans son offre technique ;
- la connaissance du contexte de la DGFiP : pour les intervenants sur les UO ECE, CPP, IAP, MCA et ISP : condition indispensable pour que ces UO soient correctement traitées. L'UO PRC permettra la prise de connaissance pour la première équipe du titulaire. En cas de remplacement d'un intervenant sur une des UO citées ci-dessus, le transfert de connaissance sera à la charge du titulaire. La DGFiP vérifiera par un questionnaire que ce transfert a bien été réalisé.

Indicateur	Stabilité des équipes
Unité	Nombre de changements au cours d'une période de 12 mois
Objectif	Pas plus d'un changement au cours d'une période de 12 mois (hors cas de force majeure)
Pénalité	Une pénalité forfaitaire de 1000 € HT par changement supplémentaire au cours des 12 derniers mois, sans mise en demeure
Prestations concernées	Pour l'ensemble des prestations couvertes par les unités d'œuvre du marché

Indicateur	Qualité des intervenants
Unité	Nombre de non-conformité aux profils types à l'occasion de l'arrivée d'un nouvel intervenant
Objectif	Pas plus d'une non-conformité à l'occasion de l'arrivée d'un nouvel intervenant pour une activité donnée (architecture, sécurité)

Pénalité	Une pénalité forfaitaire de 1000 € HT par non conformité supplémentaire, sans mise en demeure
Prestations concernées	Pour l'ensemble des prestations couvertes par les unités d'œuvre du marché

Indicateur	Connaissance du contexte de la DGFiP
Unité	Nombre de non-conformité* à la connaissance du contexte de la DGFiP
Objectif	Pas plus d'une non-conformité à l'occasion de l'arrivée d'un nouvel intervenant
Pénalité	Une pénalité forfaitaire de 1000 € HT par non conformité supplémentaire, sans mise en demeure
Prestations concernées	Pour les unités d'œuvre ECE, CPP, IAP, MCA du lot 2 et ISP, EVP du lot 3

** La non-conformité sera évaluée par l'administration lors d'un entretien*

1.10.3 Qualité des livrables

La qualité des livrables documentaires remis à l'administration s'apprécie au regard des critères suivants :

- Exigences de forme :
 - respect des modèles de documentations donnés ou approuvés par l'administration avec la version de suite logicielle détenue par l'administration ;
 - rédaction respectant les règles orthographiques et grammaticales de la langue française. Les livrables devront être exploitables et publiables en l'état, sans vérification de forme lexicale ou grammaticale de la part de la DGFiP.
- Exigences de fond :
 - couverture de l'ensemble des points et spécifications à traiter avec référence et prise en compte du contexte de la DGFiP, par rapport à l'expression des besoins de l'administration et à l'état de l'art.

Pour chaque livrable documentaire final, l'administration évalue la qualité de la livraison selon les exigences ci-dessous :

- livrable satisfaisant : toutes les exigences de fond et de forme ci-dessus sont satisfaites ;
- livrable non satisfaisant : une ou plusieurs des exigences de fond ou de forme ne sont pas satisfaites.

Un livrable final jugé « non satisfaisant » n'obtient pas le quitus de conformité et conduit le titulaire à produire un nouveau livrable sans surcoût pour l'administration. Tout retard sur le délai d'exécution généré par cette relivraison induit la pénalité standard

associée au retard dans l'exécution dont le calcul est précisé dans le CCAP.

Après deux « relivraisons » jugées « non satisfaisantes », la troisième version du livrable final qui n'obtient pas le quitus de conformité conduit simplement à « la non facturation et au non paiement par la DGFIP » de la prestation.

2 Contexte d'exécution du marché

Cette partie a pour objet de présenter les principaux processus métier du SSI et de la DTNum, pour lesquels une assistance est demandée dans le cadre du présent marché.

2.1 Présentation des réalisations d'études d'urbanisation (lot 1)

Au sein du pôle « Expérience Utilisateur » de la DTNum, **l'urbanisation du système d'information (SI) est une mission stratégique en forte visibilité**. Les équipes mènent les travaux relatifs à l'urbanisation fonctionnelle et applicative du SI et de ses composants ou modules.

La démarche d'urbanisation vise à définir, rationaliser et maîtriser l'ensemble des processus métier; elle définit la structuration cible du système d'information et organise sa transformation progressive et continue. Les travaux d'urbanisation ont pour objectif de garantir la maîtrise des processus métier et la cohérence du SI en lien avec le Schéma Directeur du Numérique (SDNum) et le Contrat d'Objectifs et de Moyens (COM) de la DGFIP. Cette démarche permet ainsi :

- d'identifier des axes de rationalisation du patrimoine applicatif pour réduire les coûts informatiques, les risques sur le SI (comme la dette technique) et les délais de mise en œuvre des projets ;
- de faciliter les parcours utilisateurs (usagers ou agents) en identifiant les ruptures applicatives et les tâches manuelles chronophages ;
- de contribuer à la transformation numérique des missions et in fine de l'amélioration des services publics portés par la DGFIP

Les études d'urbanisation fonctionnelle et applicative s'effectuent au cours de la phase d'étude préalable de tout nouveau projet, ainsi qu'en amont des évolutions envisagées du SI. Elles couvrent ainsi l'ensemble des domaines métiers et transversaux de la DGFIP (gestion fiscale, gestion publique, ressources humaines, systèmes d'information, etc.)

S'appuyant sur un ensemble de règles d'urbanisation (normes et principes) et sur la cartographie (statique) des applications de la DGFIP, les études sont conduites par des binômes de l'équipe urbanisation, en relation étroite avec les bureaux métier et les directions des projets (DP) concernés au travers de nombreuses réunions de travail. Les travaux visent à objectiver les faits et à présenter une ou plusieurs solutions avec leurs avantages et inconvénients, dans une perspective de rationalisation et de réduction des coûts.

Les études finalisées sont ensuite restituées aux responsables de la DTNum, puis font l'objet d'une présentation officielle auprès des chefs de services, des sous-directions métiers, et des DP associées.

La mission d'urbanisation revêt ainsi un caractère central au sein de la DGFiP, avec une forte visibilité, car les conclusions des travaux permettent aux hauts responsables de procéder aux arbitrages stratégiques et structurants pour les évolutions futures.

En fonction de la capacité à faire des équipes, une dizaine d'études peuvent ainsi être réalisées chaque année. La spécificité de l'urbanisation implique un rythme soutenu de réunions, nécessite également des relations avec tous les autres bureaux du SSI, les DP, et les bureaux métier et transverses de toute la DGFiP.

Des séances de travail avec d'autres ministères, partenaires, ou d'autres directions (Douanes, Tracfin, ministère de l'Intérieur, ministère de l'Écologie...) ou encore des visites opérationnelles de terrain peuvent également s'avérer nécessaires en fonction du thème de l'étude.

La conduite de l'étude implique l'élaboration d'un support de présentation dont la longueur varie entre 50 et 150 pages selon la densité et la complexité des travaux. Le support sera étayé de modélisation des processus, de tableau d'analyse ex nihilo et tout élément permettant de rendre intelligible des sujets complexes à un ensemble d'acteurs non experts des dits sujets.

La rédaction devra être synthétique sans pour autant dénaturer le sens, la gravité ou encore la réalité des sujets exposés. L'objectif étant d'éclairer les décideurs afin de leur permettre de réaliser les arbitrages stratégiques nécessaires en vue de la mise en oeuvre par les projets, des solutions cibles proposées dans les études et validées dans les instances ad hoc.

Par ailleurs, il serait intéressant d'identifier de manière prospective, au travers de méthodes éprouvées et ou d'une cartographie dynamique des processus, les axes de rationalisations qu'il conviendrait de remonter aux bureaux métier en vue de faciliter, en amont des recensements de chantiers opérationnels (RCO), les choix stratégiques des métiers.

Enfin, l'étude est présentée, conjointement avec le responsable Urbanisation du SI et le binôme ayant travaillé sur l'étude et le cas échéant avec d'autre membre de l'équipe, aux responsables hiérarchiques concernés.

2.2 Présentation des instructions d'architecture (lot 2)

2.2.1 Les instructions CAI

Le CAI¹⁴ est une instance présidée par le chef de bureau SI1 ou le chef de service SI pour les projets à forts enjeux. Cette instance vise à examiner et valider les choix applicatifs et techniques menés par les projets (hébergés sur le Cloud privé NUBO¹⁵ ou en Legacy¹⁶) en amont de la phase de développement. De manière plus générale, il vise à donner une vision 360 du projet dans toutes ses composantes (exigences, contraintes et calendrier de mise en œuvre) et à s'assurer qu'il respecte les bonnes pratiques exposées dans le cadre d'architecture de la DGFIP. L'instruction de cette instance est l'objet de l'UO IAP du paragraphe 7.4.

Les prestations de revue d'architecture pour le lot 2 (UO IAP) devront être faites dans un esprit d'impartialité si le titulaire (ou un de ses sous-traitants) est actuellement ou a été amené à participer aux phases de conception et de développement de l'application.

Le CAI s'inscrit dans le cycle de vie des projets et intervient à la fin de la phase de conception de l'architecture. Il existe 2 types de CAI : :

- **CAI général** : pour les projets à forts enjeux qui couvrent un large périmètre. Il permet de valider les grands principes d'architecture du projet ainsi que sa vision stratégique sur le long terme. Il est souvent suivi de plusieurs CAI détaillés qui traitent d'une partie spécifique du périmètre à couvrir ;
- **CAI détaillé** : pour les projets avec un périmètre plus restreint;
- **CAI ponctuel** : pour les projets qui ont besoin d'une modification à la marge de leur architecture applicative ou technique .



Cette instruction est menée par un architecte applicatif expert. Une collaboration avec l'architecte fonctionnel expert sera éventuellement nécessaire.

14 CAI : Comité d'Architecture Informatique

15 Nubo est le nom donné à l'offre de cloud privé de l'État gérée par la DGFIP, .

16 Le terme Legacy désigne les applications hébergées dans les datacenters de la DGFIP sur des serveurs physiques ou sur des plateformes virtualisées.

L'instruction débute par une phase de cadrage au cours de laquelle des ateliers sont organisés avec les acteurs du projet pour les accompagner dans la définition de l'architecture applicative et dans la complétion du dossier d'architecture générale et détaillée (DAGD). Un compte-rendu sera à fournir pour chaque réunion.

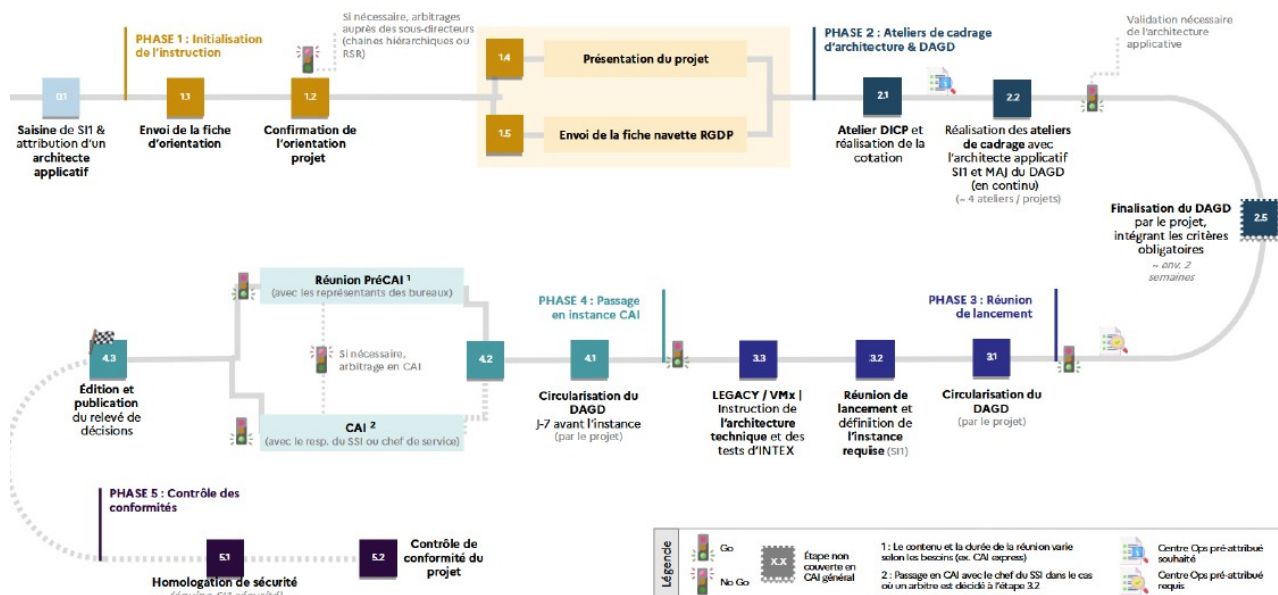
Lorsque le DAGD du projet est considéré comme finalisé, l'instruction se poursuit avec une réunion de lancement. Cette réunion a pour but d'introduire le projet et les choix d'architecture qui ont été menés lors de la phase de cadrage aux différents bureaux transverses : le bureau SI2 en charge de l'exploitation, le bureau de l'intégration en charge de l'architecture technique, de la qualification et de l'exploitabilité et le bureau SI3 en charge de la sécurité opérationnelle. Cette réunion de lancement est animée par l'équipe Architecture Applicative de la division DAN du bureau de l'architecture et des normes (SI1).

Suite à la réunion de lancement, un compte-rendu recensant les actions identifiées en séance ainsi que leurs porteurs, est transmis dans les deux jours ouvrés par l'architecte applicatif expert aux acteurs de la réunion. Dans ce compte-rendu, l'architecte applicatif expert doit recenser l'ensemble des actions à mener par le projet mais également rendre compte de l'ensemble des points structurants évoqués.

L'architecte applicatif expert est responsable de la vérification de la cohérence intégrale du support transmis par le projet (le modèle de la structure de ce support est fourni dans les annexes de ce CCTP) : conformité avec la réglementation RGPD, les normes de sécurité, le cadre d'architecture, la pile technologique, le cloisonnement applicatif, et les outils standards d'exploitabilité utilisés par la DGFiP. Ce rôle « d'auditeur » de l'architecture l'amène à rédiger une synthèse transmise à la hiérarchie une semaine avant la tenue du comité d'architecture. Cette synthèse a pour but de présenter le projet et ses particularités au chef du bureau SI1 afin de le guider dans sa prise de décision lors du CAI.

Le DAGD nécessite la contribution du bureau SI1 (sécurité applicative consistant à la réalisation de la partie exigences et contraintes en termes de sécurité – objet du second lot de ce marché), du bureau de l'intégration (architecture technique), du bureau SI3 (validation de la sécurité opérationnelle). L'architecte applicatif expert assiste le projet dans toute l'instruction et lui fait bénéficier de son expertise pour la mise en valeur des différents scénarios et de l'argumentaire permettant la prise de décision.

Si lors de la réunion de lancement, les bureaux transverses sont unanimes sur le fait que le DAGD présenté est suffisamment complet et ne soulève plus de questions, une réunion de préparation au CAI est planifiée. Cette instance se déroule de la même manière que la réunion de lancement et réunit les mêmes acteurs, elle est cependant présidée par le chef du bureau de l'architecture et des normes. À l'issue de cette instance, s'il n'y a pas de point sujet à arbitrage, le chef du bureau de l'architecture et des normes propose de demander l'accord du chef de service SI pour entériner officiellement les résultats de



« Vue d'ensemble du processus CAI pour les projets orientés Legacy/VMX »

2.2.1.1 Le Dossier d'Architecture Générale et Détaillée (DAGD)

Le Dossier d'Architecture Générale et Détaillée est un document obligatoire du projet ; Il garantit une conception alignée sur les besoins métiers, tout en définissant les principes structurants, les choix technologiques, et les modalités d'intégration de l'application au sein du SI DGFiP. Il fournit les spécifications techniques précises pour le développement, la configuration des systèmes, et la gestion des interconnexions. Il adresse les risques liés aux performances, à la sécurité et à la conformité aux normes.



« Squelette du Dossier d'Architecture Générale et Détaillée (DAGD) »

2.2.2 Les instructions FQE

Les instructions FQE¹⁷ sont réalisées par l'architecte applicatif expert. Cette procédure est un processus simplifié.

Elle vise à tracer les demandes des projets pour des évolutions d'architecture (applicative et/ou technique) peu impactantes et limitativement énumérées.

L'architecte applicatif expert en charge de l'instruction de ce dossier, doit analyser un ensemble de documents fournis par le projet afin de comprendre sa demande et d'analyser ses impacts. À ce titre, il rédige un relevé de décisions dans les 15 jours ouvrés suivant la réception d'une demande d'instruction de type FQE. Ce relevé doit éclairer la décision de la hiérarchie sur l'acceptation de cette demande (conforme à l'objectif de la FQE d'une modification de faible ampleur) ou le rejet (impact important).

Un rejet conduit nécessairement le projet à initier une instruction CAI.

2.2.3 Les instructions d'architecture fonctionnelle

Ce nouveau type d'offre de service n'est pas encore mis en œuvre. Le processus n'est à ce jour pas finalisé.

Elles sont du ressort de l'architecte fonctionnel expert.

L'objectif repose sur le besoin identifié d'un passage par une définition d'architecture fonctionnelle. Cette déclinaison et ce soutien exercés par l'architecte fonctionnel expert auprès du projet pour la définir permettront de faciliter le travail aval de l'architecte applicatif expert. Ils favoriseront en effet la transcription des besoins de l'architecture fonctionnelle vers une architecture applicative orientée services.

L'architecte fonctionnel expert intervient en amont des instructions CAI, lors de la phase de cadrage ou de la conception générale du projet.

L'architecte fonctionnel expert devra mener toutes les réunions utiles, dont chaque échange sera tracé dans des comptes-rendus. Ces ateliers ont pour but de challenger l'architecture actuelle du projet afin de l'orienter vers une architecture plus moderne et conforme aux standards en vigueur. Ils permettront par exemple d'étudier la mise en place d'API au profit de transfert de fichier ou de modules orientés services au profit d'une application monolithique.

17 FQE : Fiche de Qualification des Évolutions

2.3 Présentation du lot 3

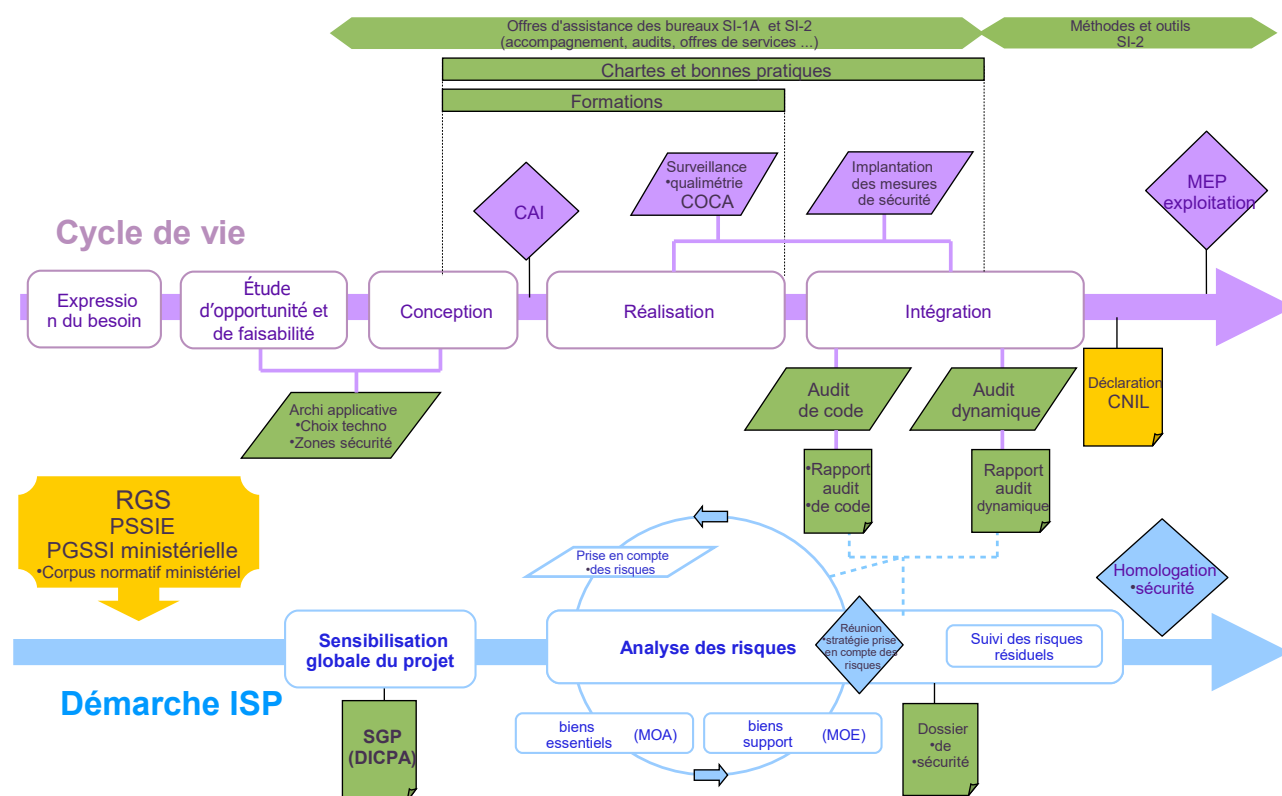
2.3.1 Présentation de la démarche d'intégration de la sécurité dans les projets (ISP)

La démarche d'intégration de la sécurité dans les projets (ISP) fait partie intégrante du cycle de vie des projets, depuis les phases d'étude amont jusqu'à la mise en production. Elle propose au projet un cadre méthodologique pour l'appréciation et le suivi des risques de sécurité du SI.

Le processus d'homologation formalise les étapes strictement nécessaires permettant de garantir une bonne appréhension, conception et mise en œuvre de la sécurité d'un système informatique.

L'autorité compétente prononce à l'issue de la vérification de ces travaux, la décision d'homologation, permettant ainsi d'attester formellement de la suffisante prise en compte de la sécurité permettant d'accepter le niveau de risques résiduels.

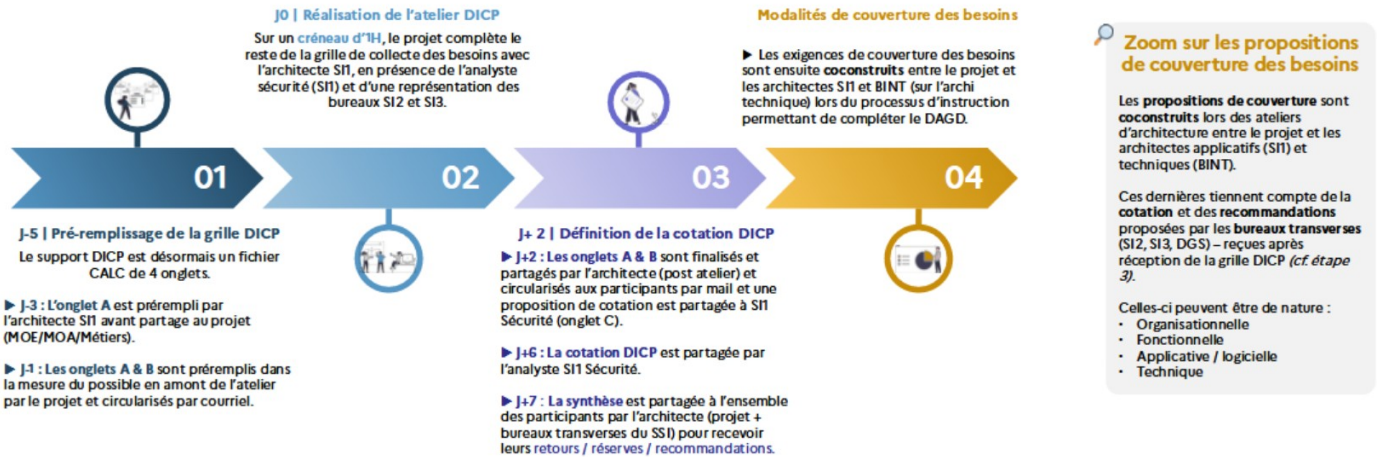
La démarche ISP se concrétise par la rédaction du dossier de sécurité du projet (DSP). Les étapes principales sont rappelées au travers du schéma ci-après¹⁸.



Étude de la sensibilité globale (cette étape est réalisée conjointement avec l'équipe d'architecture applicative qui en a la responsabilité lors de l'instruction CAI – Lot 2, et la responsabilité du respect des exigences DICP fait partie du périmètre de l'équipe SI1 SSI).

¹⁸ Les documents Recueil des risques et Plan de traitement des risques sont regroupés dans l'analyse de risques

L'étude de sensibilisation globale permet d'évaluer les exigences de sécurité du projet déclinées selon les critères de disponibilité, d'intégrité, de confidentialité et de preuve (DICP). Cette étape est impactante pour la conception de l'architecture de l'application et l'homologation de sécurité, elle doit être réalisée avant le CAI.



Appréciation des risques

Il s'agit dans un premier temps d'identifier les biens essentiels. Un bien essentiel est une information (par exemple une donnée informatique), un processus ou une fonction qui est jugé comme important pour la DGFIP, le métier qu'elle exerce, les fonctions qu'elle remplit, les tâches qu'elle accomplit.

Dans un deuxième temps, les besoins de sécurité sont exprimés par la MOA sur ces biens essentiels, en utilisant les critères DICP.

L'étape suivante consiste à identifier les risques (scénario de menace ou d'attaque, événement redouté, etc.) qui pèsent sur ces biens. Il existe quatre modes de traitement des risques identifiés :

- l'évitement, en faisant évoluer les besoins de sécurité, le périmètre initial ;
- la réduction du risque, par le biais de mesures existantes ou à mettre en œuvre ;
- le partage du risque, avec une application contributrice par exemple ;
- le maintien, c'est-à-dire accepter le risque sans mise en œuvre de mesure.

Cette expression du besoin de sécurité permettra dans un second temps d'identifier les solutions envisageables et de les qualifier par rapport aux objectifs de sécurité initiaux.

Implantation des mesures de sécurité

Il existe des fonctions de sécurité qui contribuent largement à la réalisation d'objectifs de sécurité exprimés au travers des critères DICP. Le recours à ces fonctions ou services qui sont décrits et supportés doit être privilégié par les projets.

Le cadre d'architecture expose dans son chapitre 9 les grands principes de sécurité qui s'appliquent au niveau du SI. La section présente un résumé des principes de sécurité à utiliser au niveau du projet. Dans cette approche, le chapitre 17 fournit une liste non-

exhaustive de services supportant des fonctions de sécurité disponibles au niveau du SI pour les équipes projet.

Vérification des risques

Cette phase consiste à vérifier l'implantation des mesures de sécurité, de détecter les risques résiduels (résultant d'éventuels échecs de validation) et à la validation ou la prise en compte de ceux-ci.

Les travaux de cette phase de traitement et en particulier les risques résiduels identifiés à chacune des étapes sont tracés dans le DSP¹⁹.

Des audits de sécurité menés sous le pilotage des équipes en charge de la sécurité des systèmes d'information à la DGFIP permettent notamment de détecter les éventuelles failles de sécurité des applications. Deux types d'audits techniques sont ainsi menés :

- audits de la sécurité du code des applications (audits statiques) ;
- audits de sécurité dynamiques, réalisés en environnement d'intégration.

2.3.2 Présentation de la procédure d'étude d'impact sur la vie privée à la DGFIP

Suite à la mise en œuvre du RGPD²⁰, des analyses d'impact sont menées sur les projets informatiques de la DGFIP, sous le pilotage du DRS. Ces analyses d'impact peuvent induire la réalisation d'une étude d'impact sur la vie privée (EIVP), elles sont réalisées par les équipes du DRS, une partie de l'EIVP est réalisé par l'équipe SI1 SSI et ensuite envoyé aux équipes du DRS

La procédure s'appuie sur les éléments fournis par la CNIL²¹, notamment sur le modèle de document et la base de connaissance fournis par la CNIL, qui suit les différentes étapes du processus.

19 Dossier de Sécurité Projet

20 Règlement général sur la protection des données, entré en application le 25 mai 2018

21 <https://www.cnil.fr/fr/guides-aipd>

1

La **fiche navette RGPD** (ou fiche de renseignements) doit être complétée et transmise au DGS, ce qui permettra de déterminer si une **démarche de conformité** devra être menée

Obligatoire

dgs-protection-donnees@dgrfp.finances.gouv.fr

Min. 10 jours avant la tenue du PréCAI (et après la démarche DICP)

La division CNIL de la DGS prend connaissance de la fiche et détermine la nécessité ou non d'entamer une démarche de conformité.

2

Le **DCPOD** (Dossier de Conformité à la Protection des Données) vise à démontrer que les **traitements de données personnelles** respectent les exigences légales du RGPD et de la CNIL, tout en documentant les mesures de sécurité et les processus pour protéger les droits des personnes concernées. Il constitue une **preuve de la responsabilisation** de l'organisation en matière de protection des données.

Selon projet

En fonction de la conclusion de la DGS, un DCPOD peut être lancé en parallèle de la vie du projet.

Les acteurs du processus sont les suivants :

- la cellule CNIL du DRS : pilote de la procédure ;
- le délégué à la protection des données (DPD, en anglais DPO pour « data protection officer »), positionné au Secrétariat Général : pour visa du dossier et choix de la procédure ;
- le responsable opérationnel du traitement, qui est le Chef du SSI : pour validation formelle du dossier ;
- l'équipe projet ;
- les équipes sécurité des bureaux SI1 et SI3.

Ils interviennent sur les différentes parties du document correspondant aux étapes de l'EIVP :

1) Contexte	Description du traitement et des données, détermination de la procédure à appliquer	Équipe projet, DRS
2) Principes fondamentaux	Description et évaluation des mesures portant sur les principes fondamentaux du RGPD	DRS
3) Étude des risques liés à la sécurité des données	Description et évaluation des mesures portant sur la sécurité des données, analyse des risques afférents	Équipe projet, SI1, SI3, DRS
4) Validation de l'EIVP	Synthèse des évaluations et plan d'actions, validation du dossier, suivi (demandes CNIL, événements affectant le projet après décision)	SI1, DRS, DPD, Chef du SSI

La partie 3 de l'EIVP – Étude des risques liés à la sécurité des données - contient deux sous-parties :

- mesures concourant à la protection des données personnelles ;
- appréciation des risques.

Les mesures sont détaillées selon des thèmes déterminés par la CNIL, réparties en trois catégories :

- mesures contribuant à traiter des risques liés à la sécurité des données (8 thèmes, par exemple : chiffrement, anonymisation, contrôle des accès) ;
- mesures générales de sécurité (10 thèmes, par exemple : sécurité de l'exploitation, lutte contre les logiciels malveillants, gestion des postes de travail) ; une partie des thèmes abordés dans cette partie font l'objet de fiches décrivant le standard attendu en la matière par la DGFIP. Au vu de la fiche produite, le projet doit compléter la rubrique en cas de spécificité par rapport au standard ;
- mesures organisationnelles (8 thèmes, exemple : organisation, gestion des règles, gestion des risques)

Pour chaque thème, une description des mesures mises en place ou prévues est indiquée dans une première colonne (travaux engagés). Un évaluateur estime si les mesures décrites sont acceptables ou devraient donner lieu à des mesures correctives.

mesures contribuant à traiter des risques liés à la sécurité des données	Équipe projet	SI1
mesures générales de sécurité	Équipe projet	SI3
mesures organisationnelles, cas général	Équipe projet, DRS	DRS
mesures organisationnelles / « Gestion des projets »	Équipe projet	SI1
mesures organisationnelles / « Relations avec les tiers »	Équipe projet	SI1
mesures organisationnelles / « Supervision »	Équipe projet	SI1

L'appréciation des risques portant sur la vie privée est faite sur la base de trois événements redoutés :

- accès illégitime à des données ;
- modification non désirée de données ;
- disparition de données.

Pour chacun de ces événements, sont d'abord indiquées les principales sources de risques (humaines internes et externes, non humaines), les principales menaces et les principaux impacts potentiels, en s'appuyant sur la base de connaissance téléchargeable sur le site de la CNIL (<https://www.cnil.fr/fr/PIA-privacy-impact-assessment>).

Les lignes suivantes sont remplies par les bureaux SI1 et SI3. Les principales mesures réduisant la gravité et la vraisemblance (mesures existantes ou engagées) sont remplies en se basant sur les mesures d'amélioration décrites en amont.

Les niveaux de gravité et de vraisemblance sont déterminés en s'appuyant sur la grille fournie par la CNIL dans sa base de connaissance.

Dans la partie 4 de l'EIVP - Validation de l'EIVP, le DRS et le bureau SI1 complètent la synthèse pour l'évaluation des mesures « contribuant à traiter les risques liés à la sécurité des données » conformément au contenu de la partie 3.

Le document est ensuite transmis pour avis au DPD.

Après prise en compte des éventuelles observations de ce dernier, l'EIVP est signée par le responsable du traitement.

3 Présentation du méta-modèle de la DGFIP

La présentation du méta-modèle de la DGFIP permettra au soumissionnaire de comprendre le terme de « module » utilisé dans les UO du présent cahier des charges pour évaluer leur complexité.

Un **projet** est une entité de gestion d'activités du SI ayant des objectifs, des ressources et des délais identifiés. Il est distinct d'une application qui est un outil informatique, même s'il est le seul contributeur au développement de celle-ci et porte le même nom.

Une **application** est un outil informatique qui permet de réaliser une ou plusieurs tâches ou fonctions cohérentes. Elle forme un ensemble homogène avec une MOA maître, une ou plusieurs MOE et des utilisateurs identifiés. Elle est constituée d'un ensemble de données et de traitements informatisés.

Un **projet** gère une à plusieurs applications.

Une **application** est composée de un à plusieurs modules.

Un **module** est une entité de découpage des applications qui vise à isoler des ensembles cohérents de fonctionnalités, à savoir les cas d'utilisation et services, de manière à rendre les applications plus simples, plus évolutives et à pouvoir réutiliser certains composants. Un module se décompose lui-même en plusieurs nœuds. Cette décomposition pouvant, d'une part, refléter une structuration applicative si la complexité le justifie et, d'autre part, séparer les différents éléments à déployer, à savoir les traitements, base de données et stockage.

Un **nœud** est une entité de déploiement comprenant des fichiers exécutables, suite de

composants logiciels et éléments de configuration à déployer sur un environnement d'exécution.

Le schéma suivant représente ces éléments :



Le présent marché s'arrête au niveau du nœud. Les environnements d'exécution et leur déploiement sur des matériels sont pris en charge par un autre marché portant sur l'assistance à la normalisation, conception et réalisation d'architectures dans l'environnement des technologies de l'information.

4 Explication sur le cas d'utilisation

Le nombre de cas d'utilisation (CU) est utilisé pour distinguer les niveaux de complexité de l'UO démarche ISP. Le cas d'utilisation correspond au terme du langage de modélisation unifié (UML) pour décrire une fonctionnalité du système à développer. Suite à la mise en œuvre du programme COPERNIC, les MOA de la DGFIP utilisent la méthode UML pour concevoir le système d'information.

5 Présentation des unités d'œuvre (UO) du lot 1

Les prestations génériques de Prise de Connaissance des domaines (PRC) et de Réversibilité, Transfert de Compétences (RTC) ont pour objectif une bonne transition entre des équipes sortantes et entrantes.

5.1 Unités d'œuvre du lot 1

5.1.1 UO PRC - Prise de Connaissance

5.1.1.1 Contenu de la prestation

La prestation attendue du titulaire est de prendre connaissance des éléments d'urbanisation du système d'information de la DGFIP et de son organisation générale, notamment au niveau de l'administration centrale (organigramme et compétences). Cette prestation est un préalable indispensable à la bonne réalisation des UO.

Les premiers travaux de la première équipe du titulaire dans le cadre de l'exécution du marché pourront faire l'objet d'un bon de commande de l'administration et participeront à la prise de connaissance.

L'urbanisation intervenant de manière transverse au sein de toute la DGFIP, dont l'organisation est dense et complexe, la prise de connaissance et la transmission des informations envers un prestataire constitue, pour l'équipe, **un investissement lourd qui prend 3 à 4 semaines minimum.**

5.1.1.2 Fournitures de l'administration

Cette prise de connaissance se fera via des présentations par l'administration, de la cartographie, du cadre d'architecture, de l'organisation de la DGFIP et de son administration centrale (organigramme). Elle comprendra aussi une présentation de la méthodologie mise en place au sein de la DGFIP pour simplifier, rationaliser le système d'information et mener des études d'urbanisation. Cette prise de connaissance sera complétée par une présentation synthétique de l'organisation informatique de la DGFIP et des processus concernés pour la réalisation des UO.

5.1.1.3 Livrables de la prestation

La réception de cette prestation sera prononcée par l'administration dans un délai de 4 mois calendaires. Cette réception sera basée sur les éléments fournis par l'équipe du titulaire attestant de son assimilation du contexte et des tâches à accomplir dans le cadre du présent marché. Il est attendu notamment une modélisation des processus, de la part du prestataire, représentant les différentes étapes de la méthode de conduite des études, afin de s'assurer de la bonne compréhension de la mission.

5.1.1.4 Personnels du titulaire concernés

Les personnels du titulaire concernés par cette prestation sont tous ceux qui travailleront sur les UO.

5.1.1.5 Niveau de complexité et délai de réalisation minimum

L'UO ne comprend qu'un seul niveau de complexité et concerne chaque nouveau prestataire arrivant dans l'équipe urbanisation.

Type d'UO	Niveau 1
Prise de connaissance	PRC
Délai de réalisation minimum	20 jours
Délai de validation par l'administration	4 mois

5.1.2 UO RTC - Réversibilité, Transfert de Compétences

5.1.2.1 Contenu de la prestation

L'objectif de cette prestation est de réaliser un transfert de compétences entre le titulaire et une équipe tierce désignée par la DGFIP afin de permettre un changement de prestataire sans perte de savoir-faire et de savoir.

Ce transfert de compétence peut être mis en œuvre à l'issue du présent marché.

5.1.2.2 Fournitures de l'administration

La prestation ne comporte pas de fourniture de l'administration.

5.1.2.3 Livrables de la prestation

Le titulaire doit prévoir une documentation et une démarche permettant le transfert des connaissances à cette nouvelle équipe.

Les transferts de compétences prendront la forme de séances de formation, comportant tant des aspects de présentation magistrale que des exercices pour permettre une prise en main et assurer la transmission de connaissances.

5.1.2.4 Compétences recherchées

Le transfert de compétences est assuré par les personnels du titulaire qui ont travaillé habituellement au sein de l'équipe urbanisation.

5.1.2.5 Niveau de complexité et délai de réalisation minimum

L'UO ne comprend qu'un seul niveau de complexité.

Type d'UO	Niveau 1
Réversibilité, transfert de compétence	RTC
Délai de réalisation minimum	10 jours
Délai de validation par l'administration	2 mois

5.1.3 UO Urbanisation (URB)

5.1.3.1 Contenu de la prestation

Les études d'urbanisation conduites dans le cadre de cette UO doivent permettre, en s'appuyant sur un ensemble de règles d'urbanisation maîtrisées par le prestataire, d'analyser les impacts, de définir une cible d'urbanisation et des trajectoires des migrations vers cette cible tout en s'assurant de la cohérence du système d'information, dans le cadre précisé au paragraphe 1.1 du présent CCTP.

La prestation attendue consiste à :

- définir l'urbanisation d'un domaine ou d'un sous-domaine métier du SI en fonction des besoins métier, fonctionnels et/ou techniques ;
- décrire et analyser l'existant d'une partie du système d'information sur un domaine métier donné ;
- effectuer des études d'impacts sur le système d'information pour la mise en place de nouveaux composants ou des nouveaux choix d'urbanisation ;
- définir et qualifier des cibles d'urbanisation opérationnelles, répondant aux besoins métiers et fonctionnels exprimés ;
- proposer et qualifier des trajectoires de migration d'un existant jusqu'à un système cible ;
- organiser et animer des réunions de travail avec les différents acteurs concernés par une étude (bureaux métier, maîtrise d'ouvrage, maîtrise d'œuvre, etc.)

- être garant de la bonne tenue du référentiel cartographique, en fournissant les éléments nécessaires suite à la réalisation de l'étude et en utilisant l'outil de cartographie.

La prestation a lieu dans les locaux de la DGFiP, sous le pilotage de l'équipe urbanisation de la DTNum. Selon les cas, la prestation pourra être effectuée par un binôme ou par un trinôme. Il est à noter que le mode opératoire et les besoins de l'activité induisent que plusieurs études soient menées en parallèle.

De plus des déplacements et visites dans les services centraux et territoriaux de la DGFiP seront parfois nécessaires afin d'appréhender le fonctionnement des services en charge du métier concerné dans l'étude.

5.1.3.2 Fournitures de l'administration

Dans le cadre des travaux relatifs aux études d'urbanisation, l'administration fournit :

- l'accès aux supports d'urbanisation (études, documentation et schémas existants) ;
- l'accès aux ressources « grand public » de l'intranet ULYSSE de la DGFiP ;
- l'accès à l'intranet de la DTNum permettant notamment de consulter la documentation nécessaire du système d'information ;
- l'accès à l'intranet permettant de consulter la cartographie du SI de la DGFiP.

5.1.3.3 Livrables de la prestation

Les études d'urbanisation fonctionnelles et applicatives, s'effectuent au cours de la phase d'étude préalable de tout nouveau projet, ainsi qu'en amont des évolutions envisagées du SI. Elles couvrent l'ensemble des domaines métiers et transversaux de la DGFiP (fiscalité, secteur public local, ressources humaines, etc.).

Les différents livrables seront réalisés selon les modèles fournis par la DTNum. Tous les livrables produits sont la propriété de la DGFiP.

La qualité rédactionnelle est appréciée selon les critères énoncés au §1.10 et § 2.1

La réalisation des études d'urbanisation s'articule autour de 5 grandes phases comprenant chacune plusieurs catégories d'UO et de livrables selon le profil recherché :

- **Besoin - qualification du besoin exprimé**
 - Analyse de la demande dans son contexte métier, applicatif et parfois réglementaire ;
 - Préparation et participation à ou aux réunions de cadrage ;
 - Émergence de problématiques relevant de l'urbanisation du système d'information (processus métier inadapté, rupture applicative obsolescence technologique...);
 - Proposition d'un plan d'actions pour la conduite de l'étude ;

- Rédaction de la **note de lancement** constituant un premier livrable.
- **Description existant – document du support relatif à la description et à l’analyse de l’existant**
 - Préparation, organisation et participation à des réunions avec les acteurs concernés (bureaux métier, MOA et MOE) – compte-rendus ;
 - Représentation(s) graphique(s), modélisation de processus, et commentaires d'analyse de l'existant étudié le cas échéant, tant du point de vue des processus métier que des applications concernées ;
 - Identification des points forts et des points de fragilité de l’environnement fonctionnel et applicatif étudié (ruptures applicatives, redondances fonctionnelles) ;
- **Analyse des problématiques - document du support relatif aux différentes problématiques rencontrées**
 - modélisation processus, tableaux, rappel des besoins.
- **Cibles : document du support formalisant les propositions de solutions cibles et leur qualification**
 - Préparation, participation aux réunions avec la MOA et MOE, compte-rendus ;
 - Présentation des principes d’urbanisation à retenir pour les besoins de la solution cible ;
 - Identification et priorisation des axes de rationalisation ;
 - Critères de choix, comparatif ;
 - Représentation(s) graphique(s), modélisation des processus, et commentaires d'analyse des solutions cibles envisageables, tant du point de vue des processus métier que des applications concernées ;
 - Définition d’une trajectoire de migration depuis le système existant vers le système cible ;
 - Qualification des solutions sur la base de critères pertinents.

La description de l’existant, l’analyse des problématiques et la formalisation des solutions cibles, pourront être rassemblés dans un support unique. **Ce support constituera l’étude d’urbanisation et correspondra au deuxième livrable attendu.**

- **Restitution - participation aux restitutions de l’étude devant la hiérarchie**
 - Présentation d’une partie d’un support devant un haut niveau hiérarchique ;

- Réponse aux questions ;
- Mise à jour du support suite aux remarques.

La restitution constituera le dernier livrable pour une étude donnée.

5.1.3.4 Compétences recherchées

- Une forte expérience de travaux d'urbanisation dans un contexte organisationnel et applicatif comparable à celui de la DGFiP est requise :
 - capacité à s'adapter et à intégrer l'organisation de la DGFiP ;
 - capacité à appréhender rapidement des sujets complexes.
- Par ailleurs, les compétences ci-après sont exigées dans le cadre de la conduite des études d'urbanisation :
 - expérience de plusieurs années dans le métier d'urbaniste des systèmes d'information, ou d'architecte fonctionnel des systèmes d'information;
 - expérience en architecture technique de projets notamment orientée services ;
 - qualités d'analyse et de synthèse ;
 - excellentes qualités de communication tant écrite qu'orale ;
 - capacité d'organisation et d'adaptation à différents types de publics et de niveaux hiérarchiques ;
 - aisance dans l'animation de réunion ;
 - respect et bienséance indispensables, tant envers un nombre d'interlocuteurs variés et placés à des niveaux hiérarchiques parfois très élevés qu'auprès des acteurs fréquentés au quotidien ;
 - grandes qualités relationnelles.

5.1.3.5 Niveau de complexité et délai de réalisation minimum

L'UO comprend 3 niveaux de complexité en fonction du nombre N de processus à étudier

Un processus est une suite d'activités ou d'étapes organisés de manière logique pour atteindre un objectif précis. Le processus peut être métier, fonctionnel ou technique.

Type d'UO	Complexité de l'étude	Livrables	Délai de réalisation minimum
Expression de besoin et périmètre de l'étude			
URB_B1	Simple (nombre de processus N <= 2)	Analyse de la demande Participation aux réunions Rédaction de comptes rendus	15 jours

		Rédaction de la note de lancement	
URB_B2	Moyen (nombre de processus N <= 3)	Analyse de la demande Participation aux réunions Rédaction de comptes rendus Rédaction de la note de lancement	18 jours
URB_B3	Complexe (nombre de processus N > 3)	Analyse de la demande Participation aux réunions Rédaction de comptes rendus Rédaction de la note de lancement	20 jours
Description de l'existant			
URB_DE1	Simple (nombre de processus N <= 2)	Modélisation des processus métiers, fonctionnels et applicatifs Rédaction des commentaires des processus modélisés sur le support de présentation Participation aux réunions Rédaction de comptes rendus	20 jours
URB_DE2	Moyen (nombre de processus N <= 3)	Modélisation des processus métiers, fonctionnels et applicatifs Rédaction des commentaires des processus modélisés sur le support de présentation Participation aux réunions Rédaction de comptes rendus	25 jours
URB_DE3	Complexe (nombre de processus N > 3)	Modélisation des processus métiers, fonctionnels et applicatifs Rédaction des commentaires des processus modélisés sur le support de présentation Participation aux réunions Rédaction de comptes rendus	30 jours
Analyse des problématiques			
URB_AP1	Simple (nombre de processus N <= 2)	Modélisation des processus métiers, fonctionnels et applicatifs Rédaction de commentaires des processus modélisés sur le support de présentation Réalisation de tableaux d'analyse	10 jours
URB_AP2	Moyen (nombre de processus N <= 3)	Modélisation des processus métiers, fonctionnels et applicatifs	15 jours

		Rédaction de commentaires des processus modélisés sur le support de présentation Réalisation de tableaux d'analyse	
URB_AP3	Complexe (nombre de processus N > 3)	Modélisation des processus métiers, fonctionnels et applicatifs Rédaction de commentaires des processus modélisés sur le support de présentation Réalisation de tableaux d'analyse	20 jours
Élaboration des cibles			
URB_C1	Simple (nombre de processus N <= 2)	Participation aux réunions MOA / MOE Participation aux travaux intellectuels visant à trouver la ou les cibles d'urbanisation Modélisation des processus d'urbanisation des cibles Rédaction de commentaires des processus modélisés sur le support de présentation Réalisation d'un tableau comparatif (critères métiers, d'urbanisation et fonctionnels) Proposition d'un plan de migration le cas échéant	25 jours
URB_C2	Moyen (nombre de processus N <= 3)	Participation aux réunions MOA/ MOE Participation aux travaux intellectuels visant à trouver la ou les cibles d'urbanisation Modélisation des processus d'urbanisation des cibles Rédaction de commentaires des processus modélisés sur le support de présentation Réalisation d'un tableau comparatif (critères métiers, d'urbanisation et fonctionnels) Proposition d'un plan de migration le cas échéant	30 jours
URB_C3	Complexe (nombre de processus N > 3)	Participation aux réunions MOA / MOE Participation aux travaux intellectuels visant à trouver la ou les cibles d'urbanisation Modélisation des processus d'urbanisation des cibles	35 jours

		Rédaction de commentaires des processus modélisés sur le support de présentation Réalisation d'un tableau comparatif (critères métiers, d'urbanisation et fonctionnels) Proposition d'un plan de migration le cas échéant	
Restitution de l'étude			
URB_R0	NA	Présentation en présentiel ou à distance de l'étude au top management Production de la version finale du support « orientations et actions »	5 jours
Formations des équipes internes à l'administration			
URB_F0	NA	Mise à niveau Montée en compétence Accompagnement au changement Diffusion des savoirs (nouvelles pratiques en matière d'architecture d'entreprise/cartographie) (UO mobilisable sur demande expresse de l'administration pour des besoins ciblés)	1 jour

5.1.4 UO Cartographie (CTO)

La cartographie doit permettre d'avoir une connaissance de l'ensemble des composants du SI et d'obtenir une meilleure lisibilité de celui-ci en le présentant sous différentes vues.

Dans la mesure où les outils de cartographie existants sont dispersés au sein des services informatiques, sans gouvernance commune et répondent partiellement aux besoins de la DGFIP, les travaux de cartographie conduits dans le cadre de cette UO doivent permettre, (en s'appuyant sur un ensemble de règles, normes et bonnes pratiques maîtrisées par le prestataire), de définir, concevoir et réaliser le cas échéant un ou des outils essentiels à la maîtrise du système d'information.

La prestation attendue consiste à :

- Réaliser un audit sur le sujet en s'appuyant sur des UO URB (Cf. 5.1.3)
- Proposer un PoC (Proof Of Concept) d'outil cartographique dynamique et intelligent tenant compte des contraintes techniques et de sécurité du SI DGFIP
- Concevoir une cartographie dynamique exnihilo ou à partir de briques pré-

existantes à partir d'un POC validé par la DGFiP tenant compte des contraintes techniques et de sécurité du SI DGFiP

- Assurer la mise à jour et le maintien en condition opérationnelle du produit le cas échéant

Les UO Cartographie (CTO) sont listées dans le tableau ci-après

Travaux de cartographie du SI			
CTO_MAJ	NA	Mise à jour des données de la cartographie, Travaux de veille technologique	1 jour*
CTO_BLD	NA	Construction (Build) – mise en place d'une cartographie dynamique/ Ajout de fonctionnalités/ Création de POC/ Toutes réalisations techniques relatives à la cartographie	10 jours*/ fonctionnalité
CTO_MCO	NA	Maintien en condition opérationnelle (RUN) du ou des outils de cartographie	1 jour*

* Les délais exprimés en jour sont des délais de réalisation minimum

6 Présentation des unités d'œuvre (UO) communes aux 2 lots (2 et 3)

Les prestations génériques de Prise de Connaissance des domaines (PRC) et de Réversibilité, Transfert de Compétences (RTC) ont pour objectif une bonne transition entre des équipes sortantes et entrantes.

6.1 UO PRC - Prise de Connaissance

6.1.1 Contenu de la prestation

La prestation attendue du titulaire est de prendre connaissance des éléments d'architecture et de sécurité du système d'information de la DGFiP. Cette prestation est un préalable à la bonne réalisation des UO ECE, CPP, IAP, MCA du lot 2 et ISP, EVP, CDS, ESA du lot 3.

Les ressources du titulaire qui constitueront la première équipe dans le cadre de l'exécution du marché pourront faire l'objet d'un bon de commande de l'administration et participeront à la prise de connaissance.

6.1.2 Fournitures de l'administration

Cette prise de connaissance se fera via des présentations de la cartographie, du cadre

d'architecture et de la démarche d'intégration de la sécurité dans les projets. Elle comprendra aussi une présentation de la méthodologie mise en place au sein de la DGFiP pour simplifier, rationaliser le système d'information et mettre en place des architectures standardisées. Cette prise de connaissance sera complétée par une présentation synthétique de l'organisation informatique de la DGFiP et des processus concernés pour la réalisation des UO ECE, CPP, IAP, MCA du lot 2 et ISP, EVP du lot 3.

6.1.3 Livrables de la prestation

La réception de cette prestation sera prononcée par l'administration dans un délai de 4 mois calendaires. Cette réception sera basée sur les éléments fournis par l'équipe du titulaire attestant de son assimilation du contexte et des tâches à accomplir dans le cadre du présent marché. Il est attendu notamment une modélisation des processus dont l'équipe du titulaire sera en charge.

6.1.4 Compétences recherchées

Les personnels du titulaire concernés par cette prestation sont tous ceux qui travailleront sur les UO ECE, CPP, IAP, MCA du lot 2 et ISP, EVP du lot 3.

6.1.5 Niveau de complexité et délai de réalisation minimum

L'UO ne comprend qu'un seul niveau de complexité. Elle ne couvre que la prise de connaissance de la première équipe. La prise de connaissance sera par la suite assurée par le prestataire selon les modalités décrites aux paragraphes 1.10.1 et 1.10.3.

Type d'UO	Niveau 1
Prise de connaissance	PRC
Délai de réalisation minimum	10 jours
Délai de validation par l'administration	4 mois

6.2 UO RTC - Réversibilité, Transfert de Compétence

6.2.1 Contenu de la prestation

L'objectif de cette prestation est de réaliser un transfert de compétence entre le titulaire et une équipe tierce désignée par la DGFiP afin de permettre un changement de prestataire sans perte des connaissances et du savoir-faire.

Ce transfert de compétence peut être mis en œuvre à l'issue du présent marché.

6.2.2 Fournitures de l'administration

La prestation ne comporte pas de fourniture de l'administration.

6.2.3 Livrables de la prestation

Le titulaire doit prévoir une documentation et une démarche permettant le transfert des

connaissances à cette nouvelle équipe.

Les transferts de compétence prendront la forme de séances de formation, comportant tant des aspects de présentation magistrale que des exercices pour permettre une prise en main et assurer la transmission de connaissances.

À l'issue de cette prestation, le titulaire remettra à l'administration un rapport des connaissances transférées avec les personnes formées.

6.2.4 Compétences recherchées

Le transfert de compétences est assuré par les personnels du titulaire qui ont travaillé habituellement au sein des équipes Architecture Applicative ou Sécurité du Système d'Information de la division DAN du bureau SI1 de la DGFIP.

6.2.5 Niveau de complexité et délai de réalisation minimum

L'UO comprend deux niveaux de complexité. Le premier pour des ressources ayant moins de 5 mois de présence au sein des équipes de la DGFIP et le deuxième ayant plus de 5 mois de présence.

Type d'UO	Niveau 1	Niveau 2
Réversibilité, transfert de compétence	RTC1	RTC2
Délai de réalisation minimum	10 jours	15 jours
Délai de validation par l'administration	4 mois	4 mois

7 Présentation des unités d'œuvre (UO) du lot 2

7.1 UO EPA - Expertise Ponctuelle d'Architecture

7.1.1 Contenu de la prestation

La prestation attendue a pour objectif d'aider la DGFIP à la mise en œuvre par les projets :

- de solutions d'architectures éprouvées (tant logicielles, qu'applicatives et techniques) ;
- de composants logiciels réutilisables ;
- de bonnes pratiques.

La prestation inclut les tâches suivantes :

- retours d'expérience de mises en œuvre de solutions répondant aux besoins de l'administration, dans des conditions similaires ;
- explicitation des principales alternatives pertinentes (choix technologiques, d'architecture) pour l'administration ;
- identification des bonnes pratiques d'architecture ;
- rédaction d'une note argumentée décrivant le choix préconisé, les éventuels impacts sur l'architecture du projet, au cadre d'architecture de la DGFIP, aux

normes actuellement appliquées et explicitant les raisons de ce choix ;

- rédaction d'un guide d'implémentation pour les architectes et les développeurs de l'administration.

7.1.2 Fournitures de l'administration

L'administration fournira un cadrage de l'expertise attendue. Cette UO ne nécessite pas la mise en œuvre de l'UO PRC prise de connaissance.

7.1.3 Livrables de la prestation

Les livrables attendus seront :

- document présentant les retours d'expérience pertinents ;
- note argumentée s'inscrivant dans un contexte adapté à celui de la DGFIP, décrivant le choix préconisé, et explicitant les raisons de ce choix ;
- guide d'implémentation pour les architectes et les développeurs de l'administration ;
- une ou des présentations de l'expertise (éventuellement un webinaire) ;
- comptes-rendus de toutes les réunions une semaine au plus tard après sa tenue ;
- reporting hebdomadaire sur l'état d'avancement du dossier ;

La qualité rédactionnelle sera fortement appréciée selon les critères énoncés au paragraphe 1.10.3.

Un ou des livrables intermédiaires seront nécessaires afin de s'assurer de la bonne compréhension de l'expertise attendue.

Le cadrage de l'expertise attendue pourra apporter des précisions sur les livrables.

7.1.4 Compétences recherchées

Les compétences recherchées pour cette prestation sont :

- expérience de plusieurs années en tant qu'architecte expert (applicatif, fonctionnel ou Cloud en fonction du domaine étudié et du processus) en architecture de projets orientée services (surtout REST et SOAP), aux nouvelles technologies (IA-Intelligence Artificielle, Big Data, APIM, Cloud privé...), en base de données avancées (optimisation, performance, réplication, sauvegarde...) et aux modalités d'échanges (protocoles EiDAS, OIDC...) ;
- expérience en architecture technique des services ;
- profil ayant une expertise spécifique et confirmée en architecture sur le domaine concerné (ex : Intelligence Artificielle, Data Mining, DevOps, cloud privé, open data, normes Eidas...) ;
- en privilégiant des solutions du monde libre et éventuellement documenté par la réalisation d'un prototype ;

- profil d'architecte applicatif expert, cloud expert ou fonctionnel expert correspondant au tableau du paragraphe 1.10.1 et adapté au domaine à étudier ;
- des qualités rédactionnelles et de clarté des explications ;
- de l'autonomie, savoir rendre compte et rédiger un reporting d'état d'avancement ;
- aisance à s'approprier rapidement un cadre d'architecture.
- les certifications sont appréciées.

7.1.5 Niveau de complexité et délai de réalisation minimum

L'UO ne comporte qu'un seul niveau de complexité avec un seul profil exigé : architecte expert (fonctionnel, applicatif ou Cloud en fonction du domaine étudié et du processus).

Type d'UO	Niveau 1
Expertise Ponctuelle d'Architecture	EPA
Délai de réalisation minimum	20 jours

7.2 UO ECE - Étude de Cohérence et d'Évaluation de la trajectoire de migration du SI

7.2.1 Contenu de la prestation

La prestation attendue a pour objectif d'aider la DGFIP à la mise en œuvre par les projets :

- de solutions d'architecture éprouvées et cohérentes avec la stratégie de la DGFIP ;
- de composants logiciels réutilisables en privilégiant des solutions issues du monde du libre ;
- de bonnes pratiques pour atteindre la trajectoire envisagée.

La prestation pourra être précédée d'une UO Expertise Ponctuelle d'Architecture, sans que cela soit systématique.

La prestation inclut les tâches suivantes :

- étude de cohérence entre les orientations cibles de la DGFIP et les solutions d'architecture projet, incluant d'éventuelles préconisations d'adaptations ;
- évaluation de la trajectoire de migration du SI existant vers la solution cible étudiée ;
- éventuellement la réalisation de prototypes.

7.2.2 Fournitures de l'administration

Accès au fond documentaire d'architecture de la DGFIP, à la documentation sur l'architecture du projet, à la documentation sur l'intégration de composants dans des projets existants et aux livrables logiciels de ces composants communs.

L'administration fournira un cadrage de l'expertise attendue.

7.2.3 Livrables de la prestation

Les livrables attendus seront :

- dossier d'étude de cohérence décrivant le contexte du SI et fournissant les arguments permettant de conclure sur la cohérence avec les orientations cibles de la DGFiP et de préconiser d'éventuelles adaptations ;
- dossier présentant la trajectoire de migration, les différentes étapes y menant et les recommandations pour y parvenir ;
- une ou des présentations de l'étude sont à prévoir (éventuellement un webinaire) ;
- comptes-rendus de toutes les réunions une semaine au plus tard après sa tenue ;
- reporting hebdomadaire sur l'état d'avancement du dossier.

Le cadrage de l'expertise attendue pourra apporter des précisions sur les livrables.

7.2.4 Compétences recherchées

Les compétences recherchées pour cette prestation sont :

- expérience avérée d'architecte applicatif expert en architecture de projets tout particulièrement orientée services (surtout REST et SOAP), aux nouvelles technologies (IA - Intelligence Artificielle, Big Data, APIM, Cloud privé...), en base de données avancées (optimisation, performance, réplication, sauvegarde...) et aux modalités d'échanges (protocoles EiDAS, OIDC...);
- profil d'architecte applicatif expert ou d'architecte fonctionnel expert correspondant au tableau du paragraphe 1.10.1 ;
- une expérience significative dans le domaine de la définition d'architecture : aspects méthodologiques, maîtrise des environnements internet / intranet et de la construction de modèles d'architecture en couche ;
- de l'autonomie, savoir rendre compte et rédiger un reporting d'état d'avancement ;
- des qualités rédactionnelles ;
- aisance à s'approprier rapidement un cadre d'architecture.
- les certifications sont appréciées.

7.2.5 Niveau de complexité et délai de réalisation minimum

L'UO ne comporte qu'un seul niveau de complexité avec un seul profil exigé : architecte expert (applicatif, fonctionnel ou Cloud en fonction du domaine étudié et du processus).

Type d'UO	Niveau 1
Étude de cohérence et d'évaluation de la trajectoire de migration du SI	ECE
Délai de réalisation minimum	20 jours

7.3 UO CPP - Conseils et Promotion aux Projets

7.3.1 Contenu de la prestation

La prestation attendue a pour objectif d'aider la DGFIP à la mise en œuvre par les projets :

- de solutions d'architectures éprouvées conformes au cadre d'architecture de la DGFIP ;
- de composants logiciels réutilisables issus du cadre d'architecture ;
- de bonnes pratiques recensées au sein de la DGFIP.

La prestation pourra être précédée d'une UO Expertise Ponctuelle d'Architecture, sans que cela soit systématique.

La prestation inclut les tâches suivantes :

- conseils à la définition et à la mise en œuvre de solutions et de bonnes pratiques d'architecture ayant une portée transverse ;
- actions de promotions auprès des architectes et développeurs de l'administration.

7.3.2 Fournitures de l'administration

Accès au fond documentaire d'architecture de la DGFIP, à la documentation sur l'architecture du projet, à la documentation sur l'intégration de composants dans des projets existants et aux livrables logiciels de ces composants communs.

7.3.3 Livrables de la prestation

Les livrables attendus sont :

- dossier de recommandations aux projets ;
- diaporamas de présentation ;
- réunions de promotion et comptes rendus de ces réunions.

La qualité rédactionnelle sera appréciée selon les critères énoncés au paragraphe 1.10.3.

7.3.4 Compétences recherchées

Les compétences recherchées pour cette prestation sont :

- expérience d'architecte expert en architecture de projets tout particulièrement orientée services (REST et SOAP) (IA- Intelligence Artificielle, Big Data, APIM, Cloud privé, ...), en base de données avancées (optimisation, performance, réplication, sauvegarde...);
- profil d'architecte expert (fonctionnel, applicatif, Cloud en fonction du domaine étudié ou du processus) correspondant au tableau du paragraphe 1.10.1 ;
- une compétence dans le domaine de la définition d'architecture : aspects méthodologiques, maîtrise des environnements internet / intranet et de la construction de modèles d'architecture en couche ;

- de l'autonomie, savoir rendre compte et rédiger un reporting d'état d'avancement ;
- des qualités rédactionnelles ;
- aisance à s'approprier rapidement un cadre d'architecture ;
- des qualités rédactionnelles.
- les certifications sont appréciées.

7.3.5 Niveau de complexité et délai de réalisation minimum

L'UO ne comporte qu'un seul niveau de complexité avec un seul profil exigé : architecte expert (fonctionnel, applicatif ou Cloud en fonction du domaine étudié et du processus).

Type d'UO	Niveau 1
conseils et promotion	CPP
Délai de réalisation minimum	20 jours

7.4 UO IAP - Instructions d'Architecture des Projets

7.4.1 Contenu de la prestation

La prestation attendue consiste à assister les projets dans l'instruction des CAI et des FQE.

Le titulaire devra assister opérationnellement les projets dans leurs choix d'architecture vis-à-vis de la cible DGFIP. Il commentera et explicitera les règles d'architecture à appliquer par les projets. Il devra également analyser l'architecture des projets et instruire les problématiques.

Il apportera une aide au projet sur la coordination de plusieurs acteurs à la production d'un support de présentation nécessaire à la tenue du CAI. Les acteurs principaux sont les bureaux SI2 pour l'aspect exploitation, SI3 pour la sécurité opérationnelle et le bureau de l'intégration pour l'architecture technique, la qualification et l'exploitabilité. Il participera aux différentes réunions, réalisera les comptes-rendus, une synthèse, un relevé de décisions suite au comité préparatoire au CAI ou dans le cas d'une FQE auquel s'ajoutera un relevé d'actions pour le CAI.

Les déroulés d'une instruction CAI et FQE sont décrits dans les paragraphes 2.1.1 et 2.1.2.

7.4.2 Fournitures de l'administration

L'administration fournira au préalable :

- une ébauche du dossier d'architecture du projet ainsi que le contexte du projet ;
- les contraintes techniques inhérentes aux infrastructures et aux orientations de l'architecture technique ;
- les éléments servant à construire les hypothèses pour les calculs des unités de dimensionnement ;
- accès au fond documentaire d'architecture de la DGFIP.

7.4.3 Livrables de la prestation

- Comptes-rendus des réunions (dont la réunion de lancement de l'instruction CAI) ;
- Tableau des actions dans les deux jours après la réunion de lancement mis à jour au fur et à mesure de l'avancée du projet ;
- Relevé d'actions suite à une préparation CAI non transformée en CAI une semaine au plus tard après la tenue de la réunion ;
- Assistance du projet à la coordination des acteurs et à la mise en œuvre des actions demandées relevant de l'architecture applicative et/ou fonctionnelle ;
- Reporting hebdomadaire de l'état d'avancement des instructions ;
- Synthèse avant la tenue de la préparation CAI ou le CAI au plus tard une semaine avant la tenue de la réunion ;
- Relevé de décisions suite au CAI ;

La qualité rédactionnelle sera appréciée selon les critères énoncés au paragraphe 1.10.3.

7.4.4 Compétences recherchées

Les compétences recherchées sont les suivantes :

- capacité à s'intégrer rapidement dans l'organisation et le fonctionnement d'une administration publique ;
- capacité à appréhender rapidement des sujets complexes ;
- une compétence d'architecte applicatif expert (cf. tableau du paragraphe 1.10.1) dans le domaine de la définition d'architecture : aspects méthodologiques, maîtrise des environnements internet / intranet et de la construction de modèles d'architecture en couches, architecture orientée services (REST et SOAP) ;
- une compétence dans la conduite d'entretiens (ordre du jour à constituer impérativement à chaque réunion suivie d'un compte-rendu) ;
- une aisance dans la communication orale adaptée au niveau hiérarchique des interlocuteurs ;
- une autonomie et une capacité à gérer simultanément plusieurs dossiers présentant un niveau de maturité variable ;
- une capacité à s'adapter au projet et dans la répartition de ses tâches (parallélisation importante des tâches et des dossiers à prévoir) à s'organiser pour respecter impérativement les échéances des livrables (savoir anticiper, prioriser en accord avec la hiérarchie et alerter) ;
- en veille technique en continu pour être au fait de l'état de l'art et des orientations SI de la DGFIP ;
- de grandes qualités rédactionnelles ;
- de grandes qualités relationnelles.

7.4.5 Niveau de complexité et délai de réalisation minimum

La complexité de l'étude demandée est fonction de l'environnement dans lequel se situe le projet, de son importance stratégique et du volume attendu d'interventions.

L'UO comprend 3 niveaux de complexité, avec un seul profil exigé : architecte applicatif expert.

Une instruction FQE est considérée à l'instar d'un CAI de niveau 1 : simple.

Niveau 1 : simple	
Description du contexte	Projet particulier aux besoins de la DGFiP, sans lien avec des services stratégiques ou dans le cadre d'une instruction FQE
Utilisation de services transverses	Projet n'utilisant pas de services transverses du SI
Volume indicatif d'interventions	Moins de 5 réunions avec les personnes participant à cette instruction
Délai de validation des livrables finaux par l'administration	1 mois
Niveau 2 : moyen	
Description du contexte	Projet défini comme connexe par rapport aux services considérés comme stratégiques
Utilisation des services transverses	Projet utilisant éventuellement certains des services transverses du SI
Volume indicatif d'interventions	Moins de 12 réunions avec les personnes participant à cette instruction
Délai de validation des livrables finaux par l'administration	3 mois
Niveau 3 : complexe	
Description du contexte	Projet considéré comme stratégique : référentiel, service transversal, applicatif avec de nombreuses interactions avec d'autres projets, projet central par rapport au SI. Projet répondant à des contraintes de performance particulièrement importantes
Utilisation des services transverses	Projet utilisant nécessairement certains des services transverses du SI
Volume indicatif d'interventions	Moins de 20 réunions avec les personnes participant à cette instruction
Délai de validation des livrables finaux par l'administration	4 mois

Les UO seront codifiées de la façon suivante :

Type d'UO	Niveau 1 : simple	Niveau 2 : moyen	Niveau 3 : complexe
Instruction CAI	IAP1	IAP2	IAP3
Délai de réalisation minimum	20 jours	25 jours	30 jours

7.5 UO MCA - Mise à jour du Cadre d'Architecture applicative

7.5.1 Contenu de la prestation

La prestation attendue consiste à mettre à jour les documents fixant le cadre d'architecture de la DGFIP. Cette mise à jour se fera à partir de plusieurs documents techniques provenant de différentes sources. Elle pourra être issue de conclusions suite à la mise en œuvre de prototypes dans le cas des architectes Cloud. Une mise à jour des supports de formation sera demandé en parallèle, si nécessaire.

7.5.2 Fournitures de l'administration

Accès au fond documentaire d'architecture de la DGFIP.

7.5.3 Livrables de la prestation

Défini dans le bon de commande, il pourra s'agir, en plus d'un des documents du cadre d'architecture, d'une fiche technique, d'une note, d'un guide ou de la mise à jour d'un support de formation.

La qualité rédactionnelle sera appréciée selon les critères énoncés au paragraphe 1.10.3.

7.5.4 Compétences recherchées

Les compétences recherchées pour cette UO sont les suivantes :

- une compétence générale dans la problématique associée aux nouvelles technologies ;
- une compétence d'architecte expert (applicatif, fonctionnel ou Cloud en fonction du domaine étudié) (cf. tableau du paragraphe 1.10.1) dans le domaine de la définition d'architecture : aspects méthodologiques, maîtrise des environnements internet / intranet et de la construction de modèles d'architecture en couches, de l'architecture orientée services SOAP et REST, du Cloud privé ;
- qualités rédactionnelles, de synthèse et pédagogiques dans le cas de la rédaction d'un support de formation.

7.5.5 Niveau de complexité et délai de réalisation minimum

L'UO ne comporte qu'un seul niveau de complexité avec un seul profil exigé : architecte

expert (applicatif, fonctionnel ou Cloud en fonction du domaine étudié).

Type d'UO	Niveau 1
Mise à jour du cadre d'architecture applicative	MCA
Délai de réalisation minimum	20 jours

8 Présentation des unités d'œuvre (UO) du lot 3

8.1 UO ISP - Intégration de la Sécurité dans les Projets

8.1.1 *Contenu de la prestation*

La prestation attendue consiste à accompagner l'équipe projet dans la démarche d'appréciation des risques menée dans le cadre d'une homologation de sécurité.

Le cadre réglementaire : RGS v2, PSSIE, PGSSI, Décret n° 2022-513 du 8 avril 2022

- Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives (AA) et entre les AA.
- Décret n° 2010-112 du 2 février 2010, qui donne les modalités d'applications de l'ordonnance pour la partie relative à la sécurité, et qui officialise le RGS.
- L'homologation de sécurité est affirmée comme un axe majeur de la politique de sécurité de l'Etat (PSSI-E, juillet 2014) et de la politique ministérielle de la sécurité numérique (PMSN décembre 2023).

L'analyse est effectuée sur la base des entretiens menés avec l'équipe projet et éventuellement le métier, ainsi que sur la documentation fournie par le projet. Elle intégrera également les réponses techniques apportées par les équipes transverses du SI de la DGFIP qui pourraient être sollicitées.

La réalisation de la prestation s'articule actuellement autour de quatre phases auxquelles participe l'intervenant en charge de l'analyse :

- Phase de collecte :
 - étude de la documentation du projet ;
 - réalisation d'entretiens avec les équipes métiers et/ou projet pour l'étude des biens essentiels ;
 - réalisation d'entretiens avec l'équipe MOE pour l'étude des biens support ;
 - compléments d'informations, notamment avec les équipes transverses du SI de la DGFIP.
- Phase de synthèse et de rédaction :
 - prise en compte du formalisme et de la méthode de rédaction de la grille d'analyse de risques.
- Réunion de stratégie de prise en compte des risques :

- présentation aux représentants de l'équipe projet des risques attachés au système d'information, pour prise de décision par celle-ci quant à la stratégie à adopter pour chacun de ces risques.

Ces phases de réalisation seront amenées à évoluer durant l'année 2026.

La prestation sera menée selon les indications et les consignes données lors de la phase de cadrage par la DGFIP qui pourra contrôler le travail réalisé tout au long de celle-ci.

Il n'est pas autorisé de connexion à distance entre les sites du titulaire et de l'administration.

Le titulaire fournira une clé chiffrée pour le stockage des informations relatives aux applications faisant l'objet de l'analyse de risques.

8.1.2 Fournitures de l'administration

L'administration fournira au préalable tout document utile à la réalisation de la prestation, par exemple :

- les caractéristiques du SI ;
- le support du comité d'architecture informatique (CAI) du projet, qui intègre une analyse globale de la sécurité de ce dernier ;
- les spécifications générales et détaillées de l'application ;
- l'architecture fonctionnelle de l'application ;
- les normes et documents de référence, notamment en termes de sécurité.

Elle fournira également le modèle des livrables.

8.1.3 Livrables de la prestation

Les livrables principaux attendus pour la prestation sont une grille d'analyse de risques, ainsi que le support de la commission d'homologation, qui seront réalisés selon le modèle fourni par le bureau d'architecture et des normes.

Il sera complété par :

- le suivi des différentes réunions assorti d'un CR succinct de chacune ;
- une note de synthèse présentant le contexte et les différentes contraintes relevées, la justification des options retenues de même que celles rejetées ;
- une fiche mentionnant tous les livrables de la prestation.

La qualité rédactionnelle sera appréciée selon les critères énoncés au paragraphe 1.10.3.

Par ailleurs, des points d'étape seront effectués par l'administration sur les jalons essentiels de l'analyse risque, portant notamment sur :

- le respect du formalisme méthodologique de la DGFIP ;
- le traitement des problématiques abordées par l'analyse de risques ;
- le respect des calendriers définis lors du cadrage de la prestation.

8.1.4 Compétences recherchées

L'intervenant chargé de la prestation devra avoir un profil d'expert en risques numériques (cf. paragraphe 1.10.1), et une solide expérience en matière de gestion des risques des systèmes d'information, en particulier, de manière opérationnelle, quant à la réalisation d'analyses de risques d'applications.

Cette activité nécessite des compétences particulières :

- une maîtrise de la méthode EBIOS 2010 , EBIOS RM et des normes ISO 27001, 27002 et 27005 ;
- une compétence technique dans le domaine de la sécurité, notamment dans des environnements internet / intranet ;
- une maîtrise du cadre juridique de la sécurité s'appliquant à l'administration, et notamment : RGPD, loi informatique et libertés, eIDAS, RGS, PSSI Etat ;
- une expérience des problématiques d'urbanisation et d'architecture applicative et technique est un plus, les aspects métiers, fonctionnels, applicatifs et techniques devant être bien compris.

Elle demande en outre les qualités suivantes :

- l'autonomie et l'esprit d'initiative ;
- la capacité d'analyse et de synthèse ;
- les qualités rédactionnelles pour la clarté et la logique des exposés ;
- les qualités de communication attendues pour les échanges avec les équipes projets métier ;
- la capacité à échanger avec l'équipe interne en partageant ses connaissances et son expérience.

8.1.5 Niveau de complexité et délai de réalisation minimum

Une unité d'œuvre correspondra à la réalisation d'une analyse de risques, de trois niveaux de complexité possible. La complexité des analyses de risques sera déterminée en tenant compte des critères suivants : complexité métier et fonctionnelle, complexité de l'architecture.

Une unité d'œuvre correspondant à l'analyse de risques d'une application, elle sera impérativement réalisée par un seul intervenant possédant le profil expert en risques numériques.

Niveau 1 : simple	
Description du contexte	Un nombre de cas d'utilisation concernés allant de 1 à 10
Délai de validation des livrables finaux	1 mois
Niveau 2 : moyen	

Description du contexte	Un nombre de cas d'utilisation concernés allant de 11 à 20
Délai de validation des livrables finaux	2 mois
Niveau 3 : complexe	
Description du contexte	Un nombre de cas d'utilisation concernés supérieur à 21
Délai de validation des livrables finaux	3 mois

Les UO seront codifiées de la façon suivante :

Type d'UO	Niveau 1 : simple	Niveau 2 : moyen	Niveau 3 : complexe
Intégration de la sécurité dans les projets	ISP1	ISP2	ISP3
Délai de réalisation minimum	10 jours	20 jours	40 jours

8.2 UO SGP - Étude de sensibilité globale du projet

8.2.1 Contenu de la prestation

La prestation attendue consiste à accompagner les équipes projet dans l'expression des besoins de sécurité selon les critères de disponibilité, d'intégrité, de confidentialité, de gestion de la preuve de contrôle, lors d'une phase de sensibilisation générale du projet à la sécurité (SGP), qui fait l'objet d'un examen en Comité d'architecture informatique (CAI).

L'analyse est effectuée sur la base d'un entretien mené avec le métier et/ou l'équipe projet et sur la documentation fournie par le projet.

8.2.2 Fournitures de l'administration

L'administration fournira au préalable tout document utile à la réalisation de la prestation, par exemple :

- les caractéristiques du SI ;
- le support du précédent comité d'architecture informatique (CAI) du projet ;
- les spécifications générales de l'application ;
- l'architecture fonctionnelle de l'application ;
- les normes et documents de référence, notamment en termes de sécurité.

Elle fournira également le modèle des livrables.

8.2.3 Livrables de la prestation

Le livrable attendu pour la prestation est un support sous forme de diapositives qui sont intégrées au support de la réunion du Comité d'architecture informatique (CAI). Le livrable sera réalisé selon le modèle fourni par le bureau d'architecture et des normes.

La qualité rédactionnelle sera appréciée selon les critères énoncés au paragraphe 1.10.3.

8.2.4 Compétences recherchées

L'intervenant chargé de la prestation devra avoir un profil de consultant en sécurité des SI (cf. paragraphe 1.10.1).

Cette activité nécessite des compétences particulières :

- une compétence technique dans le domaine de la sécurité, notamment dans des environnements internet / intranet ;
- une bonne connaissance du cadre juridique de la sécurité s'appliquant à l'administration, et notamment : RGPD, loi informatique et libertés, eIDAS, RGS, PSSI Etat ;

Elle demande en outre les qualités suivantes :

- l'autonomie et l'esprit d'initiative ;
- la capacité d'analyse et de synthèse ;
- les qualités rédactionnelles pour la clarté et la logique des exposés ;
- les qualités de communication attendues pour les échanges avec les équipes projets et métiers ;

8.3 Niveau de complexité et délai de réalisation minimum

Les UO seront codifiées de la façon suivante :

Type d'UO	Niveau 1
Etude de sensibilité globale du projet	SGP
Délai de réalisation minimum	10 jours

8.4 UO EVP - Étude d'impact sur la vie privée

8.4.1 Contenu de la prestation

La prestation attendue consiste à accompagner les équipes projet dans la démarche d'appréciation des risques menée dans le cadre d'une étude d'impact sur la vie privée (EIVP).

Ces études sont menées sous le pilotage de l'équipe CNIL du DRS et ont pour objectif d'évaluer les risques liés à la sécurité des données des applications la DGFIP et, le cas échéant, de proposer des mesures correctives.

L'analyse est effectuée sur la base des entretiens menés avec l'équipe projet et éventuellement le métier, ainsi que sur la documentation fournie par le projet.

La prestation comprend l'évaluation ou la rédaction des parties de l'EIVP visées aux articles 3.1.1, 3.1.2, 3.1.3 (exclusivement pour les trois rubriques « Gestion des projets », « Relations avec les tiers » et « Supervision »), 3.2 et 4.1.2 du DC-POD.

La réalisation de la prestation s'articule autour de trois phases auxquelles participe l'intervenant en charge de l'analyse :

- Phase de collecte :
 - étude du document transmis par le DRS (DC-POD) ;
 - réalisation d'entretiens avec l'équipe projet et éventuellement métier ;
- Phase d'analyse ;
 - évaluation des mesures proposées pour assurer la protection des données à caractère personnel, proposition des scénarios de menaces ;
 - compléments éventuels à recueillir auprès de l'équipe projet ;
- Phase de synthèse et de rédaction :
 - prise en compte du formalisme et de la méthode de rédaction du DC-POD.

La prestation sera menée selon les indications et les consignes données lors de la phase de cadrage par la DGFIP qui pourra contrôler le travail réalisé tout au long de celle-ci.

Il n'est pas autorisé de connexion à distance entre les sites du titulaire et de l'administration.

Le titulaire fournira une clé chiffrée pour le stockage des informations relatives aux applications faisant l'objet de l'étude d'impact sur la vie privée.

8.4.2 Fournitures de l'administration

L'administration fournira au préalable le dossier pré-rempli (DC-POD). Le cas échéant, elle pourra fournir tout document utile à la réalisation de la prestation, par exemple :

- les caractéristiques du SI ;
- le support du comité d'architecture informatique (CAI) du projet, qui intègre une analyse globale de la sécurité de ce dernier ;
- les spécifications générales et détaillées de l'application ;
- l'architecture fonctionnelle de l'application ;
- les normes et documents de référence, notamment en termes de sécurité.

8.4.3 Livrables de la prestation

Les livrables attendus pour chacune des EIVP qui sera réalisée sont les suivants :

- le document DC-POD complété sur les parties 3.1, 3.2 et 4.1.2 ;
- en cas d'entretien avec le projet, un compte-rendu synthétique des échanges incluant le cas échéant un plan d'actions.

8.4.4 Compétences recherchées

L'intervenant chargé de la prestation devra avoir un profil d'expert en risques numériques (cf. paragraphe 1.10.1), et une solide expérience en matière de gestion des risques des systèmes d'information et de conformité à la réglementation relative à la protection des données à caractère personnel.

Cette activité nécessite ainsi des compétences approfondies en matière de connaissances

techniques sur le domaine de la protection des données, tout particulièrement dans le cadre du RGPD.

Elle demande en outre les qualités suivantes :

- l'autonomie et l'esprit d'initiative ;
- la capacité d'analyse et de synthèse ;
- les qualités rédactionnelles pour la clarté et la logique des exposés ;
- les qualités de communication attendues pour les échanges avec les équipes projets métier ;
- la capacité à échanger avec l'équipe interne en partageant ses connaissances et son expérience.

8.4.5 Niveau de complexité et délai de réalisation minimum

Une unité d'œuvre correspondra à la réalisation d'une étude d'impact sur la vie privée (EIVP), de trois niveaux de complexité possible. La complexité des EIVP sera déterminée en tenant compte des critères suivants : complexité métier et fonctionnelle, complexité de l'architecture.

Une unité d'œuvre correspondant à l'EIVP d'un traitement automatisé donnée, elle sera impérativement réalisée par un seul intervenant possédant le profil expert en risques numériques.

Niveau 1 : simple	
Description du contexte	Un nombre de cas d'utilisation concernés allant de 1 à 10
Délai de validation des livrables finaux	1 mois
Niveau 2 : moyen	
Description du contexte	Un nombre de cas d'utilisation concernés allant de 11 à 20
Délai de validation des livrables finaux	2 mois
Niveau 3 : complexe	
Description du contexte	Un nombre de cas d'utilisation concernés supérieur à 21
Délai de validation des livrables finaux	3 mois

Les UO seront codifiées de la façon suivante :

Type d'UO	Niveau 1 : simple	Niveau 2 : moyen	Niveau 3 : complexe
Étude d'impact sur la vie privée	EVP1	EVP2	EVP3
Délai de réalisation minimum	10 jours	20 jours	40 jours

8.5 UO CDS - Contrôle Développement et audits Sécurité

8.5.1 Contenu de la prestation

La prestation attendue consiste à réaliser des audits de sécurité :

- un contrôle de code sur la sécurité applicative ou audit de sécurité du code
- un audit de tests d'intrusion ou pentest
- un audit de configuration
- un audit sécurité d'architecture
- un audit organisationnel et physique

Comme indiqué dans le CCAP au paragraphe 9.3, une clause s'applique en cas de conflits d'intérêt sur les prestations du Lot 3, notamment lors de la réalisation des audits sécurité : audit de sécurité du code, audit de configuration, audit de tests d'intrusion, d'audit sécurité d'architecture, d'audit organisationnel et physique. Par exemple si le titulaire de rang 1 a participé au développement ou à l'architecture du projet ;

Les prestations d'audit de sécurité pour le lot 3 (UO CDS) devront être réalisées par un titulaire ayant la qualification PASSI (prestataires d'audit de la sécurité des systèmes d'information : https://cyber.gouv.fr/sites/default/files/document/PASSI_Referentiel-exigences_v2.2.pdf qui est PASSI pour les 5 portées d'audit ci-après : audit d'architecture, audit de configuration, audit de code source, tests d'intrusion, audit organisationnel et physique.

Les audits de sécurité du code ont pour objet d'évaluer le respect des bonnes pratiques de sécurité et d'identifier les failles de sécurité présentes dans le code du projet. L'analyse se base notamment sur l'état de l'art et les différents Top Ten OWASP.

L'évaluation est effectuée sur la base des sources du projet, les entretiens avec l'équipe projet et les documents d'architecture dont le Comité d'architecture Informatique (CAI) du projet. L'audit de code est réalisé à l'aide d'outillage d'analyse de sécurité du code et il est complété par une analyse visuelle du code source de l'application.

Le niveau de criticité de chaque vulnérabilité est évalué en utilisant un système d'évaluation standardisé appelé Common Vulnerability Scoring System (CVSS) qui est basé sur des critères objectifs et mesurables.

L'environnement technique est l'environnement Java/J2EE en architecture web et n/tier et l'environnement PHP.

Le périmètre de la prestation couvre également, si nécessaire, l'ingénierie du développement et l'architecture du code.

L'audit de sécurité statique pourra être complété par la réalisation de tests d'intrusion, qui seront menés sur une plate-forme d'intégration ou de pré-production.

L'audit de configuration consiste à évaluer le niveau de conformité et/ou de sécurité de la configuration des dispositifs matériels et logiciels déployés au sein d'un système

d'information.

L'audit d'architecture consiste à évaluer le niveau de conformité et/ou de sécurité d'un système d'information notamment par l'analyse des choix de positionnement et de mise en œuvre des dispositifs matériels et logiciels déployés en son sein. L'audit d'architecture peut être étendu aux interconnexions du système d'information audité avec des réseaux tiers, et notamment Internet.

L'audit organisationnel et physique consiste à évaluer le niveau de conformité et/ou de sécurité de la gouvernance, des politiques et procédures de sécurité mises en œuvre pour assurer le maintien en conditions de sécurité du système d'information audité.

L'audit organisationnel et physique peut couvrir l'évaluation de la protection des ressources physiques du système d'information audité comme par exemple les systèmes de contrôle d'accès physique, de détection d'intrusions physiques, de vidéoprotection, de prévention des risques naturels (incendie, inondations, etc.).

Le code source des applications auditées ne pourra en aucun cas être externalisé ni même analysé en dehors des locaux de la DGFIP. En particulier, il n'est pas autorisé de connexion à distance entre les sites du titulaire et de l'administration.

Le titulaire fournira une clé chiffrée pour le stockage des informations relatives aux applications auditées.

La réalisation de la prestation d'audit s'articule autour de quatre phases auxquelles participe l'auditeur :

- Phase de collecte :
 - réalisation d'entretiens avec les responsables techniques de projets (équipes projet et développement), notamment lors de la réunion de lancement de l'audit (d'une durée d'une heure environ) ;
 - étude de la documentation du projet ;
 - analyse manuelle et/ou automatique des sources et de la documentation du projet audité.
- Phase d'analyse et d'interprétation :
 - analyse des failles relevées par l'outillage, comprenant une analyse manuelle complémentaire aux résultats fournis par le logiciel d'analyse de code ;
 - étude des actions à mener par le projet pour corriger ces failles.
- Phase de rédaction :
 - prise en compte du formalisme et de la méthode de rédaction des rapports, y compris pour l'évaluation des vulnérabilités décelées (CVSS 3) ;
 - réalisation du rapport, des fiches de risques et du plan d'actions.
- Phase de communication :
 - la communication intervient tout au long de l'audit, tant avec les équipes

internes qu'avec le responsable du projet audité lors de la phase de lancement, de l'entretien et de la présentation des livrables lors de la réunion de restitution de l'audit (d'une durée de l'ordre de 1h30).

La prestation sera menée selon les indications et les consignes données par la DGFIP qui pourra contrôler le travail réalisé tout au long de celle-ci.

8.5.2 Fournitures de l'administration

L'administration fournit au préalable :

- les caractéristiques du SI ;
- les programmes sources ;
- les urls des plateformes, des comptes de tests ;
- la documentation projet, par exemple :
 - les spécifications générales et détaillées de l'application
 - l'architecture fonctionnelle de l'application
 - le dossier de conception de l'application
- les normes et documents de référence.

Elle fournira également les modèles des livrables, ainsi que le référentiel utilisé pour la constitution des fiches de vulnérabilités.

8.5.3 Livrables de la prestation

Trois livrables sont attendus pour chaque audit réalisé :

- une liste des fiches de risques ;
- un rapport d'audit ;
- une proposition de plan d'action.

L'ensemble des constatations faites, au cours des échanges et des analyses menées à partir du dépôt de source et de la documentation, est détaillé dans des fiches de risque. L'objectif de ce document est, pour chaque point de risque identifié :

- d'évaluer le niveau de criticité du risque identifié en utilisant la méthode CVSS v3 ; ce niveau est évalué dans une échelle de 0 à 10 ;
- de commenter le risque identifié en le mettant en perspective avec les enjeux du projet ;
- de préconiser la mise en œuvre d'actions visant à réduire les risques du projet. Ces actions sont nuancées par rapport au contexte du projet.

Le rapport expose, à la date de l'audit, une synthèse des sujets couverts en détail par les fiches de risque.

Les actions préconisées dans les fiches de risque sont rappelées dans le plan d'actions qui inclut une estimation du niveau d'effort correspondant.

Les différents livrables seront réalisés selon les modèles fournis par le bureau SI1.

La qualité rédactionnelle sera appréciée selon les critères énoncés au paragraphe 1.10.3.

8.5.4 Compétences recherchées

L'auditeur devra avoir un profil d'auditeur de code (cf. paragraphe 1.10.1), et donc une solide expérience en matière d'audit de sécurité de code applicatif.

Cette activité d'audit nécessite des compétences particulières :

- les qualités techniques liées à la sécurité des développements ;
- les qualités techniques liées aux technologies et aux outils de l'environnement Java/J2EE.

Elle demande en outre les qualités suivantes :

- l'autonomie et l'esprit d'initiative ;
- la capacité d'analyse et de synthèse ;
- les qualités rédactionnelles pour la clarté et la logique des exposés ;
- les qualités de communication attendues pour les échanges avec les équipes projets, notamment pour la restitution de l'audit ;
- la capacité à échanger avec l'équipe interne en partageant ses connaissances et son expérience.

L'auditeur devra également avoir une très bonne connaissance opérationnelle des langages utilisés (Java et PHP) et des filières techniques DGFIP (Linux, Spring, Struts, JSF, Hibernate...).

8.5.5 Niveau de complexité et délai de réalisation minimum

La prestation comprendra une ou plusieurs unités d'œuvre correspondant à la réalisation d'autant d'audits, de trois niveaux de complexité possible. La complexité des audits sera déterminée en tenant compte des critères suivants : architecture complexe, utilisation de frameworks externes à l'application nécessitant des investigations complémentaires.

Une unité d'œuvre correspondant à l'audit de sécurité d'une application, elle sera impérativement réalisée par un seul auditeur possédant le profil d'auditeur de sécurité du code.

Niveau 1 : simple	
Description du contexte	Un nombre de modules applicatifs concernés allant de 1 à 5.
Niveau 2 : moyen	
Description du contexte	Un nombre de modules applicatifs concernés allant de 6 à 10.

Niveau 3 : complexe	
Description du contexte	Un nombre de modules applicatifs concernés supérieur à 10.

Les UO seront codifiées de la façon suivante :

Type d'UO	Niveau 1 : simple	Niveau 2 : moyen	Niveau 3 : complexe
Contrôle développement et audits sécurité	CDS1	CDS2	CDS3
Délai de réalisation minimum	7 jours	10 jours	15 jours

8.6 UO ESA – Étude de sécurité applicative

8.6.1 Contenu de la prestation

La prestation attendue consiste à réaliser pour le bureau SI1 une étude portant sur une problématique de sécurité applicative.

L'étude pourra inclure pour le domaine étudié :

- une description de l'état de l'art ;
- une étude de l'existant quant au système d'information de la DGFIP. L'analyse d'un panel représentatif d'applications de différentes filières de la DGFIP pourra être réalisée ;
- la stratégie de mise en œuvre, en prenant en compte :
 - la faisabilité et le coût de la mise en place pour les différentes filières et projets existants.
 - la valeur ajoutée en termes de sécurité ajoutée au SI.
- Les bonnes pratiques à mettre en œuvre dans le contexte du SI de la DGFIP.

La prestation sera menée selon les indications et les consignes données par la DGFIP lors de la réunion de lancement, qui pourra contrôler le travail réalisé tout au long de celle-ci.

8.6.2 Fournitures de l'administration

L'administration fournit au préalable :

- les caractéristiques du SI ;
- le cas échéant, les programmes sources d'un panel d'applications de la DGFIP sélectionnées par le bureau SI1 ;
- les normes et documents de référence.

8.6.3 Livrables de la prestation

Les livrables attendus pour la prestation seront définis lors de la réunion de lancement. Ils

pourront comprendre :

- un rapport des travaux d'analyse avec les éléments suivants (étude d'opportunité et analyse d'impact, recommandations techniques de mise en place, etc.) ;
- une présentation des résultats de l'étude sous forme de diaporama.

Les différents livrables seront réalisés selon les modèles fournis par le bureau SI1.

La qualité rédactionnelle sera appréciée selon les critères énoncés au paragraphe 1.10.3.

8.6.4 Compétences recherchées

L'auditeur devra avoir un profil d'expert en sécurité applicative (cf. paragraphe 1.10.1).

Cette activité d'audit nécessite des compétences particulières :

- des connaissances approfondies en matière de sécurité des SI ;
- les qualités techniques liées à la sécurité des développements ;
- les qualités techniques liées aux technologies et aux outils de l'environnement Java/J2EE et PHP.

Elle demande en outre les qualités suivantes :

- l'autonomie et l'esprit d'initiative ;
- la capacité d'analyse et de synthèse ;
- les qualités rédactionnelles pour la clarté et la logique des exposés ;
- les qualités de communication attendues pour les échanges avec des équipes projets ;
- la capacité à échanger avec l'équipe interne en partageant ses connaissances et son expérience.

L'auditeur devra également avoir une très bonne connaissance opérationnelle des langages utilisés (Java et PHP) et des filières techniques DGFIP (Linux, Spring, struts, JSF, Hibernate).

8.6.5 Niveau de complexité et délai de réalisation minimum

L'UO ne comporte qu'un seul niveau de complexité avec un seul profil exigé : expert en sécurité applicative.

Type d'UO	Niveau 1
Étude de sécurité applicative	ESA
Délai de réalisation minimum	30 jours

9 Présentation des unités d'œuvre (UO) du lot 4

9.1 GR – Gestion des risques informatiques

9.1.1 Contenu de la prestation

La prestation attendue consiste à fournir à l'équipe sécurité les licences des outils de

gestion des risques afin de couvrir le périmètre de ses missions :

- homologation de sécurité (méthode EBIOS-RM) ;
- traitement du risque informatique (registre de risques informatiques) ;

Ces outils de sécurité doivent être dans la mesure du possible qualifiés par l'ANSSI et sous la forme uniquement de logiciel on premise déployable dans un environnement Linux.

Conformément à la politique ministérielle de la sécurité numérique (PMSN de 2023), les solutions logicielles retenues devront faire l'objet d'une homologation de sécurité par la DGFIP. Dans cet optique, le titulaire fournira l'ensemble des documentations nécessaires à ces homologations (politique de sécurité des systèmes d'information (PSSI), documentations techniques, rapport d'audit, documentations d'exploitation et autres documents susceptibles de constituer un apport méthodologique) et le cas échéant les certificats de conformité.

Les besoins de sécurité seront spécifiés lors de la phase de définition et la documentation relative à la sécurité devra être communiquée lors de la phase de restitution.

La réalisation de la prestation s'articule autour des six phases suivantes :

- Phase de sourcing :
 - étude du cahier des charges relatif a un nouveau besoin d'outil de gestion de risques
 - réalisation d'entretiens avec l'équipe sécurité pour affiner la compréhension du besoin d'outils
 - présentation à l'équipe de sécurité des différents outils de gestion des risques relatif au besoin définit dans la première phase avec une évaluation de sécurité conforme aux exigences de la DGFIP
- Phase de POC :
 - En fonction de la restitution, une phase d'expérimentation pourra être demandée afin de qualifier l'outil par l'équipe de sécurité.
- Phase d'acquisition :
 - Dans le cas où l'équipe de sécurité retient une solution décrite dans la phase de restitution, le prestataire fournira les droits d'utilisation/binaire de cet outil intégrant les différents éléments (licences, clefs d'utilisation, documentation, conformité de sécurité, support et maintenance) .
- Phase de renouvellement :
 - Cette phase sert à renouveler les licences existantes.
- Phase d'intégration et configuration :

- Il s'agit d'une phase optionnelle permettant à l'équipe de sécurité d'avoir une assistance sur la configuration, l'intégration et le déploiement de la solution logicielle.
- Phase de formation :
 - Il s'agit d'une phase optionnelle. A la demande de l'équipe de sécurité, en fonction des besoins ou des conclusions de la phase de restitution, une phase d'accompagnement ou de formation pourra être demandée permettant d'acquérir les compétences nécessaires à l'utilisation de l'outil.

La prestation sera menée selon les indications et les consignes données lors de la phase de cadrage par la DGFIP qui pourra contrôler le travail réalisé tout au long de celle-ci.

Il n'est pas autorisé de connexion à distance entre les sites du titulaire et de l'administration.

Le titulaire fournira une clé/conteneur chiffré pour le stockage des informations relatives aux applications faisant l'objet de l'analyse de risques.

9.1.2 Fournitures de l'administration

L'administration fournira au préalable tout document utile à la réalisation de la prestation, par exemple :

- les caractéristiques du SI
- le cahier des charges de l'outil
- les contraintes techniques et de sécurité applicables au choix de l'outil de sécurité
- les normes et documents de référence (qualification ANSSI, ISO, ...), notamment en termes de sécurité
- Les résultats d'audit de sécurité
- la procédure de maintien de condition de sécurité (correctifs de sécurité,...)

9.1.3 Livrables de la prestation

Les livrables principaux attendus pour la prestation sont :

- Le rapport d'évaluation et la grille d'analyse des outils par rapport au cahier des charges fourni ;
- les licences et droit d'utilisation de l'outil de sécurité ;
- les documentations techniques et fonctionnelles de l'outil de sécurité ;
- le cas échéant les supports de formation liés à l'accompagnement sur site ;
- la documentation de conformité de sécurité.

9.1.4 Liste des outils existants

Outils de gestion des risques informatiques	
Outils	Editeurs
Arimes (licence)	ADACIS
AGRIOS (licence)	ADACIS

La liste des outils ci-dessus n'est pas exhaustive, le titulaire pourra préconiser d'autres outils propriétaires et/ou opensources différents répondant mieux au besoin.

9.1.5 Niveau de complexité et durée de réalisation

La prestation comprendra une ou plusieurs unités d'œuvre correspondant aux différentes prestations d'acquisition, de trois niveaux de complexité possible. La complexité des logiciels ou solution SAAS à acquérir sera déterminée en tenant compte des critères suivants : stockage de données sensibles, intégration dans le système d'information, conformité et dossier de sécurité (ANSSI, SOC, ...).

Niveau 1 : simple	
Description du contexte	Type de licence on premise Intégration dans le SI : faible Données sensibles : oui Conformité : documentation éditeur Niveau homologation : simplifiée
Niveau 2 : moyen	
Description du contexte	Type de licence on premise Intégration dans le SI : moyenne ou complexe Données sensibles : oui Conformité : référentiel de base (ISO) Niveau homologation : intermédiaire
Niveau 3 : complexe	
Description du contexte	Type de licence on premise Intégration dans le SI : moyenne ou complexe Données sensibles : oui Conformité : référencé ANSSI Niveau homologation : renforcée

Les UO seront codifiées de la façon suivante pour les phases hors acquisition de licence:

Il s'agit d'une durée minimale incompressible pour réaliser les différentes phases.

GR - Gestion des risques informatiques

Type d'UO	UO	N : simple	N2 : moyen	N3 : complexe
Sourcing	GR-S	5 jours	10 jours	20 jours
POC	GR-P	10 jours	20 jours	60 jours
Acquisition	Voir annexe financière			
Renouvellement				
Installation et configuration	GR-I	2 jours	3 jours	5 jours
Formation	GR-F	2 jours	5 jours	10 jours

9.2 OF – Outils de formation

9.2.1 Contenu de la prestation

La prestation attendue consiste à fournir à l'équipe sécurité les licences des outils de formation afin de couvrir le périmètre de ses missions :

- outils de formation avancée de sécurité (hackTheBox, OWASP, ...)

Ces outils de formation peuvent être sous la forme de logiciels on premise déployable dans un environnement linux et windows ou sous la forme d'offre SAAS.

Conformément à la politique ministérielle de la sécurité numérique (PMSN de 2023), les solutions logicielles retenues pourront faire l'objet d'une homologation de sécurité par la DGFiP. Dans l'affirmative, le titulaire fournira l'ensemble des documentations nécessaires à ces homologations (politique de sécurité des systèmes d'information (PSSI), documentations techniques, rapport d'audit, documentations d'exploitation,...) et dans le cas échéant les certificats de conformité.

Les besoins de sécurité seront spécifiés lors de la phase de définition et la documentation relative à la sécurité devra être communiquée lors de la phase de restitution.

La réalisation de la prestation s'articule autour des six phases suivantes :

- Phase de sourcing :
 - étude du cahier des charges relatif a un nouveau besoin d'outil de formation.
 - réalisation d'entretiens avec l'équipe sécurité pour affiner la compréhension du besoin d'outils.

- présentation à l'équipe de sécurité des différents outils de sécurité relatif au besoin défini dans la première phase avec une évaluation de sécurité conforme aux exigences de la DGFIP.
- Phase de POC :
 - En fonction de la restitution, une phase d'expérimentation pourra être demandée afin de qualifier l'outil par l'équipe de sécurité.
- Phase d'acquisition :
 - Dans le cas où l'équipe de sécurité retient une solution décrite dans la phase de restitution, le prestataire fournira les droits d'utilisation/binaire de cet outil intégrant les différents éléments (licences, clefs d'utilisation, documentation, conformité de sécurité, support et maintenance) .
- Phase de renouvellement :
 - Cette phase sert à renouveler les licences existantes acquises ou non via ce marché.
- Phase d'intégration et configuration :
 - Il s'agit d'une phase optionnelle permettant à l'équipe de sécurité d'avoir une assistance sur la configuration, l'intégration et le déploiement de la solution logicielle.
- Phase de formation :
 - Il s'agit d'une phase optionnelle. A la demande de l'équipe de sécurité, en fonction des besoins ou des conclusions de la phase de restitution, une phase d'accompagnement ou de formation pourra être demandée permettant d'acquérir les compétences nécessaires à l'utilisation de l'outil.

La prestation sera menée selon les indications et les consignes données lors de la phase de cadrage par la DGFIP qui pourra contrôler le travail réalisé tout au long de celle-ci.

Il n'est pas autorisé de connexion à distance entre les sites du titulaire et de l'administration.

Le titulaire fournira une clé/conteneur chiffré pour le stockage des informations relatives aux applications faisant l'objet de l'analyse de risques.

9.2.2 Fournitures de l'administration

L'administration fournira au préalable tout document utile à la réalisation de la prestation, par exemple :

- les caractéristiques du SI
- le cahier des charges de l'outil
- les contraintes techniques et de sécurité applicables au choix de l'outil de sécurité

- les normes et documents de référence (qualification ANSSI, ISO, ...), notamment en termes de sécurité
- Les résultats d'audit de sécurité
- la procédure de maintien de condition de sécurité (correctifs de sécurité,...)

9.2.3 Livrables de la prestation

Les livrables principaux attendus pour la prestation sont :

- Le rapport d'évaluation et la grille d'analyse des outils par rapport au cahier des charges fourni ;
- les licences et droit d'utilisation de l'outil de sécurité ;
- les documentations techniques et fonctionnelles de l'outil de sécurité ;
- le cas échéant les supports de formation liés à l'accompagnement sur site ;
- la documentation de conformité de sécurité.

9.2.4 Liste des outils existants

Outils de formations de sécurité	
Outils	Editeurs
HackTheBox (licence)	HTB
Owasp Juice Shop (libre)	MIT Licence
Gandalf AI (libre)	Lakera

La liste des outils ci-dessus n'est pas exhaustive, le titulaire pourra préconiser d'autres outils propriétaires et/ou opensources différents répondant mieux au besoin.

9.2.5 Niveau de complexité et délai de réalisation minimum

La prestation comprendra une ou plusieurs unités d'œuvre correspondant aux différentes prestations d'acquisition, de trois niveaux de complexité possible. La complexité des logiciels ou solution SAAS à acquérir sera déterminée en tenant compte des critères suivants : stockage de données sensibles, intégration dans le système d'information, conformité et dossier de sécurité (ANSSI, SOC, ...).

Niveau 1 : simple	
Description du contexte	Type de licence on premise / SAAS Intégration dans le SI : faible Conformité : documentation éditeur

	Niveau homologation : simplifiée
Niveau 2 : moyen	
Description du contexte	Type de licence on premise / SAAS Intégration dans le SI : moyenne Conformité : référentiel de base (ISO) Niveau homologation : simplifiée
Niveau 3 : complexe	
Description du contexte	Type de licence on premise / SAAS Intégration dans le SI : complexe Conformité : référentiel de base (ISO) Niveau homologation : simplifiée

Les UO seront codifiées de la façon suivante pour les phases hors acquisition de licence:
Il s'agit d'un délai de réalisation minimum pour réaliser les différentes phases.

OF - Outils de formation

Type d'UO	UO	N1 : simple	N2 : moyen	N3 : complexe
Sourcing	OF-S	5 jours	8 jours	10 jours
POC	OF-P	5 jours	8 jours	10 jours
Acquisition	Voir annexe financière			
Renouvellement				
Installation et configuration	OF-I	1 jour	2 jours	3 jours
Formation	OF-F	2 jours	5 jours	8 jours

9.3 OS – Outils de sécurité

9.3.1 Contenu de la prestation

La prestation attendue consiste à fournir à l'équipe sécurité les licences des outils de sécurité afin de couvrir le périmètre de ses missions :

- audit de sécurité (SAST, DAST, ...)

Ces outils de sécurité peuvent être sous la forme de logiciels on premise déployable uniquement dans un environnement linux et exceptionnellement sous windows.

Conformément à la politique ministérielle de la sécurité numérique (PMSN de 2023), les

solutions logicielles retenues pourront faire l'objet d'une homologation de sécurité par la DGFIP. Dans l'affirmative, le titulaire fournira l'ensemble des documentations nécessaires à ces homologations (politique de sécurité des systèmes d'information (PSSI), documentations techniques, rapport d'audit, documentations d'exploitation,...) et dans le cas échéant les certificats de conformité.

Les besoins de sécurité seront spécifiés lors de la phase de définition et la documentation relative à la sécurité devra être communiquée lors de la phase de restitution.

La réalisation de la prestation s'articule autour des six phases suivantes :

- Phase de sourcing :
 - étude du cahier des charges relatif a un nouveau besoin d'outil de formation.
 - réalisation d'entretiens avec l'équipe sécurité pour affiner la compréhension du besoin d'outils.
 - présentation à l'équipe de sécurité des différents outils de sécurité relatif au besoin définit dans la première phase avec une évaluation de sécurité conforme aux exigences de la DGFIP.
- Phase de POC :
 - En fonction de la restitution, une phase d'expérimentation pourra être demandée afin de qualifier l'outil par l'équipe de sécurité.
- Phase d'acquisition :
 - Dans le cas où l'équipe de sécurité retient une solution décrite dans la phase de restitution, le prestataire fournira les droits d'utilisation/binaire de cet outil intégrant les différents éléments (licences, clefs d'utilisation, documentation, conformité de sécurité, support et maintenance) .
- Phase de renouvellement :
 - Cette phase sert à renouveler les licences existantes acquises ou non via ce marché.
- Phase d'intégration et configuration :
 - Il s'agit d'une phase optionnelle permettant à l'équipe de sécurité d'avoir une assistance sur la configuration, l'intégration et le déploiement de la solution logicielle.
- Phase de formation :
 - Il s'agit d'une phase optionnelle. A la demande de l'équipe de sécurité, en fonction des besoins ou des conclusions de la phase de restitution, une phase d'accompagnement ou de formation pourra être demandée permettant d'acquérir les compétences nécessaires à l'utilisation de l'outil.

La prestation sera menée selon les indications et les consignes données lors de la phase de cadrage par la DGFIP qui pourra contrôler le travail réalisé tout au long de celle-ci.

Il n'est pas autorisé de connexion à distance entre les sites du titulaire et de l'administration.

Le titulaire fournira une clé/conteneur chiffré pour le stockage des informations relatives aux applications faisant l'objet de l'analyse de risques.

9.3.2 Fournitures de l'administration

L'administration fournira au préalable tout document utile à la réalisation de la prestation, par exemple :

- les caractéristiques du SI
- le cahier des charges de l'outil
- les contraintes techniques et de sécurité applicables au choix de l'outil de sécurité
- les normes et documents de référence (qualification ANSSI, ISO, ...), notamment en termes de sécurité
- Les résultats d'audit de sécurité
- la procédure de maintien de condition de sécurité (correctifs de sécurité,...)

9.3.3 Livrables de la prestation

Les livrables principaux attendus pour la prestation sont :

- Le rapport d'évaluation et la grille d'analyse des outils par rapport au cahier des charges fourni ;
- les licences et droit d'utilisation de l'outil de sécurité ;
- les documentations techniques et fonctionnelles de l'outil de sécurité ;
- le cas échéant les supports de formation liés à l'accompagnement sur site ;
- la documentation de conformité de sécurité.

9.3.4 Liste des outils existants

Outils d'audits de sécurité et DevSecOps pour les projets	
Checkmarx SAST (licence)	Checkmarx
Sonarcube (licence)	SonarSource
Owasp Dependency Check (libre)	OWASP – Apache 2 Licence
Owasp ZAP (libre)	Checkmarx – Apache 2.0
Trivy version Community (libre)	Aqua Security - Apache 2.0
Gitleaks (libre)	MIT Licence

Checkov (libre)	Prisma Cloud - Apache Licence 2.0
-----------------	-----------------------------------

La liste des outils ci-dessus n'est pas exhaustive, le titulaire pourra préconiser d'autres outils propriétaires et/ou opensources différents répondant mieux au besoin.

9.3.5 Niveau de complexité et délai de réalisation minimum

La prestation comprendra une ou plusieurs unités d'œuvre correspondant aux différentes prestations d'acquisition, de trois niveaux de complexité possible. La complexité des logiciels ou solution SAAS à acquérir sera déterminée en tenant compte des critères suivants : stockage de données sensibles, intégration dans le système d'information, conformité et dossier de sécurité (ANSSI, SOC, ...).

Niveau 1 : simple	
Description du contexte	Type de licence on premise Intégration dans le SI : faible Données sensibles : non Conformité : documentation éditeur Niveau homologation : simplifiée
Niveau 2 : moyen	
Description du contexte	Type de licence on premise Intégration dans le SI : moyenne ou complexe Données sensibles : oui Conformité : référentiel de base (ISO) Niveau homologation : intermédiaire
Niveau 3 : complexe	
Description du contexte	Type de licence on premise Intégration dans le SI : moyenne ou complexe Données sensibles : oui Conformité : référencé ANSSI Niveau homologation : renforcée

Les UO seront codifiées de la façon suivante pour les phases hors acquisition de licence:
Il s'agit d'un délai de réalisation minimum pour réaliser les différentes phases.

AS - Outils de sécurité

Type d'UO	UO	N1 : simple	N2 : moyen	N3 : complexe
Sourcing	AS-S	5 jours	10 jours	20 jours
POC	AS-P	10 jours	20 jours	60 jours
Acquisition	Voir annexe financière			
Renouvellement				
Installation et configuration	AS-I	2 jours	3 jours	5 jours
Formation	AF-F	2 jours	5 jours	10 jours

9.4 Formations à la sécurité informatique

La DGFIP souhaite se doter d'un panel de formations certifiantes à destination de ses agents sur un ensemble de sujets relatifs à la sécurité informatique. Il appartient au titulaire de proposer des formations à distance et en présentiel dans les locaux du titulaire sur les sujets suivants :

Hacking éthique
Sécurité applicative/web
Tests d'intrusion
Audit de configuration système
Sécurité de l'active directory
Sécurité Kubernetes
Sécurité de l'IA/LLM
Containers
Nouvelles vulnérabilités et techniques
d'attaques/veille sécurité
Audit de configuration
terraform/ansible (IaC)
Ebios RM

Ces formations devront être dispensées selon les standards édictés par l'ANSSI et permettront aux agents d'obtenir des certifications reconnues soit par ce même organisme ou soit par un organisme reconnu dans le domaine de la sécurité.

Le titulaire doit remplir l'annexe financière relative aux formations en indiquant un prix HT par personne, que la formation soit dispensée à distance ou en présentiel.

Le titulaire devra détailler le catalogue de formation disponible et le cas échéant les organismes sur lesquels il s'appuie pour les dispenser.

Pour les formations en présentiel, les agents DGFIP peuvent se voir dispenser une formation inter-entreprise et/ou spécifique aux agents DGFIP dans la mesure où le nombre d'agents suffit à organiser pour ces derniers une session en propre.

10 Annexes

Les annexes au présent CCTP se composent des documents suivants, contenus dans le fichier « **Annexes-CCTP-urba-archi-sécu.zip** ». Ces documents sont accessibles sur demande²² du candidat.

10.1 Périmètre des missions et organisation de la Direction générale des Finances publiques

- « **nid_13319_descriptif.pdf** » : présente de manière plus complète la mission et l'organisation de la DGFIP ;
- « **nid_13109_organigramme_dgfip.pdf** » : présente l'organigramme de la DGFIP.
- « **Présentation_et_Organigramme_de_la_DTNUM** » : présente l'organigramme de la DTNUM.

10.2 Cadre d'architecture et exemple d'études

Documents importants fixant le cadre d'architecture de la DGFIP :

- « **Cadre d'architecture V3.0** » : présente le cadre de cohérence commun à toutes les architectures. Ce document didactique, accessible à tous les acteurs projet (MOE, MOA) expose les principes, les démarches applicables et les outils disponibles pour fabriquer des applications en prenant en compte les exigences et les contraintes (interopérabilité, ergonomie, sécurité, ...) auxquelles les applications de la DGFIP doivent répondre. Il se prolonge par un guide qui décrit les cibles à privilégier en identifiant les critères de choix des architectures à appliquer par les projets ;
- « **C_ARCHI_cartographie_2012_annexe_V1.0.pdf** » : L'objectif du document est d'effectuer une cartographie du système d'information de la DGFIP selon les différents niveaux d'architecture (métier, fonctionnel, applicatif et technique) ;
- « **Etude_CaaS_V1.2.pdf** » : étude réalisée en août 2023 pour mesurer les impacts et la démarche pour l'utilisation de la conteneurisation dans le contexte du cloud privé DGFIP ;
- « **DGFIP_Etude_SpringIntegration_rapport_V1.0.pdf** » : étude réalisée en décembre 2024 ayant pour objectif principal d'évaluer l'utilisation de Spring Integration pour le développement de modules applicatifs Java dans le contexte spécifique de la

22 Cf. modalités dans le règlement de la consultation

DGFIP ;

- « **C_ARCHI_demarche_dimensionnement_V1.0.pdf** » : ce document décrit la démarche de dimensionnement formalisée avec le bureau des infrastructures et de la sécurité pour faciliter le passage de l'architecture applicative à l'architecture technique dans le cadre de la stratégie technique retenue pour le SI.

10.3 Modèles

- « **Modèle DAGD.pdf** » : plan type du dossier d'architecture générale et détaillée ;

10.4 Cadre pour le développement

- La charte OSD « **Charte_OSD-2.0.1.pdf** » (Organisation et Structuration des Développements) propose un cadre d'organisation de l'ensemble des ressources d'un projet (code, tests, documentation, libraires externes, ...) afin d'unifier les pratiques de développement et d'intégration tout en garantissant la pérennité et la maintenabilité des applications livrées. La charte OSD constitue un référentiel précis pour conduire les opérations de contrôle liées à la recette technique ;
- **Le guide de règles et de recommandations relatives au développement d'applications de sécurité en Java JavaSec** : <http://www.ssi.gouv.fr/agence/publication/securite-et-langage-java/>, ainsi que les **préconisations du Open Web Application Security Project (OWASP) en sécurité applicative** : <http://www.owasp.org> sont les documents de référence pour la sécurité applicative. Ces documents s'inscrivent dans la démarche globale de sécurité du SSI et représentent l'état de l'art dans ce domaine. Ils ont pour but de sensibiliser les chefs de projet à la prise en compte de la sécurité dans le développement des applications. Ils couvrent l'aspect programmation, en présentant les attaques les plus courantes (injection SQL, Cross Site Scripting, ...) assorties des parades appropriées ;
- « **1-Lombok-presentation-26.1.pdf** » : ce document présente le cadriciel Lombok qui est l'outillage principal pour le développement des applications Java de la DGFIP ;
 - « **6-Lombok-les composants techniques-26-1.pdf** » : annexe cadriciel Lombok ;
 - « **7-Lombok-les composants metiers-26-1.pdf** » : annexe cadriciel Lombok.

10.5 Accessibilité et ergonomie

- Le Référentiel Général d'Accessibilité pour les Administrations est destiné à définir, en France, les modalités techniques d'accessibilité, notamment sur les services en ligne de l'État. Cette problématique concerne les personnes souffrant d'un handicap visuel, moteur, auditif, cognitif voire même de handicaps multiples. Le site de référence pour récupérer la dernière version du RGAA est <http://www.numerique.gouv.fr/publications/rgaa-accessibilite/> ;

10.6 Conditions de sécurité

- « **Clausier_travail_local_distant_télétravail.odt** » : cette annexe décrit les contraintes techniques imposées au prestataire pour ses postes de travail locaux ou distants.