

POUVOIR ADJUDICATEUR**Agence Française de Développement (AFD)**

5 rue Roland Barthes
75598 PARIS Cedex 12

OBJET DE LA CONSULTATION N° ASO-2026-0266**Intitulé du marché :**

Prestations de fourniture de service de Tierce Maintenance Applicative - Périmètre
VERSO (et autres applications Bonita)

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES
(C.C.T.P.) – Annexe 4 - Cadre Technologique -
Compléments**

Fiche d'évolution			
Révision	Date	Objet de l'évolution	Auteur
1.0	18/09/2026	Création du document	Julien GEERAERT Fabien TALMA Carla ROCHE

1. Présentation de l'annexe	5
1.1. Rôle du système d'information	7
1.2. Périmètre fonctionnel couvert.....	7
1.3. Enjeux structurants du SI	7
2. Gouvernance du système d'information et principes directeurs	7
2.1. Principes généraux de gouvernance du SI	7
2.2. Organisation générale de la gouvernance	8
2.3. Principes directeurs d'urbanisation du SI.....	8
2.4. Méthodes projets et modes de conduite des projets SI	9
3. Architecture globale du système d'information (vue macro)	9
3.1. Principes structurants d'architecture.....	9
3.2. Découpage macro du système d'information.....	9
<i>Canaux et interfaces utilisateurs</i>	<i>9</i>
<i>Applications métiers et progiciels</i>	<i>10</i>
<i>Données, référentiels et pilotage</i>	<i>10</i>
<i>Services transverses mutualisés.....</i>	<i>10</i>
4. Interopérabilité et intégration applicative	10
4.1. Principes généraux d'interopérabilité.....	10
4.2. Cadre général d'intégration applicative	10
4.3. Typologie des échanges applicatifs.....	10
4.4. Gestion des erreurs, supervision et traçabilité	11
5. Gestion des données	11
5.1. Principes généraux de gestion des données	11
5.2. Gouvernance et responsabilité sur la donnée	11
6. Hébergement et infrastructures	11
6.1. Principes généraux d'hébergement	11
6.2. Environnements et séparation des usages	12
6.3. Environnement de travail des utilisateurs	12
6.4. Mutualisation et standardisation des infrastructures	12
6.5. Accès aux infrastructures et sécurité d'hébergement	13
6.6. Exploitation, supervision et maintenabilité	13
6.7. Sauvegarde et protection des données	13
7. Réseaux et connectivité.....	13
7.1. Principes généraux de connectivité	13
7.2. Interconnexion des sites et accès au SI	14
7.3. Accès distants et mobilité	14
7.4. Flux applicatifs et principes de communication.....	14
7.5. Segmentation et cloisonnement réseau.....	14
7.6. Résilience et performance des accès	15
8. Gestion des identités et des accès (IAM)	15
8.1. Principes généraux de gestion des identités	15
8.2. Authentification et Single Sign-On	15
8.3. Modèle d'habilitation et gestion des droits	15
8.4. Intégration des applications au dispositif IAM	16
8.5. Exigences techniques d'intégration (niveau conceptuel)	16
<i>Mécanismes SSO supportés.....</i>	<i>16</i>
<i>Mode 1 – Contrôle d'accès « simple »</i>	<i>17</i>
<i>Mode 2 – Contrôle d'accès « par permissions ».....</i>	<i>17</i>
8.6. Comptes techniques et accès privilégiés.....	17
9. Sécurité du système d'information.....	18

9.1.	Principes généraux de sécurité	18
9.2.	Gouvernance et cadre de référence sécurité.....	18
9.3.	Sécurité des accès et des identités	18
9.4.	Sécurité applicative	18
9.5.	Protection des données.....	19
9.6.	Journalisation, supervision et gestion des incidents	19
9.7.	Sécurité des infrastructures et de l'hébergement.....	19
10.	Contraintes réglementaires et conformité	19
10.1.	Cadre réglementaire général.....	19
10.2.	Protection des données à caractère personnel.....	19
10.3.	Sécurité du SI et gestion des risques	20
10.4.	Continuité d'activité et résilience opérationnelle	20
10.5.	Traçabilité, auditabilité et contrôles	20
10.6.	Localisation des données et recours à des tiers	20
10.7.	Responsabilités et engagements des prestataires	21
11.	Exploitation et maintien en conditions opérationnelles,	21
11.1.	Principes généraux d'exploitation	21
11.2.	Séparation des responsabilités Build / Run	21
11.3.	Supervision et exploitation courante.....	21
11.4.	Gestion des incidents et des anomalies	21
11.5.	Maintenance corrective et évolutive	21
11.6.	Gestion des changements et des mises en production.....	22
11.7.	Documentation et support à l'exploitation	22
12.	Cycle de vie applicatif et gestion de l'obsolescence,	22
12.1.	Principes généraux de maîtrise du cycle de vie.....	22
12.2.	Phases du cycle de vie applicatif.....	22
12.3.	Maintenabilité et évolutivité des solutions.....	23
12.4.	Gestion de l'obsolescence.....	23
12.5.	Réversibilité et fin de vie	23
13.	Attentes vis-à-vis des prestataires,	23
13.1.	Respect du cadre SI et des principes d'architecture	23
13.2.	Qualité des solutions et des livrables	23
13.3.	Sécurité et gestion des risques	24
13.4.	Capacité d'intégration et d'exploitabilité.....	24
13.5.	Organisation, méthodes et collaboration	24
13.6.	Pérennité, évolutivité et réversibilité	24

1. Présentation de l'annexe

La présente annexe a pour objet de fournir aux prestataires une présentation synthétique et structurée du système d'information (SI) de l'AFD, afin de leur permettre :

- ▶ De comprendre le contexte général dans lequel s'inscrit la consultation ;
- ▶ D'identifier les principes structurants, contraintes et exigences applicables aux solutions proposées ;
- ▶ De faciliter la formulation de réponses pertinentes, réalistes et compatibles avec l'environnement existant.

Cette annexe constitue un document de cadrage général, elle n'a pas vocation à décrire de manière exhaustive ou opérationnelle le SI existant.

Les informations qu'elle contient ont pour finalité de définir les exigences techniques applicables et de permettre au TITULAIRE d'établir une réponse conforme, complète et cohérente au regard des attentes de l'AFD.

Les éléments de réponse fournis par le TITULAIRE devront être strictement alignés avec le « Cadre de Référence Technique » (annexe 7) et ses compléments, lesquels constituent des documents contractuels de référence.

Le TITULAIRE pourra, le cas échéant, formuler des propositions d'évolution ou d'adaptation portant sur les architectures applicative, logicielle et/ou technique. Toute proposition de cette nature devra être :

- ▶ Explicitement identifiée ;
- ▶ Dûment justifiée et argumentée ;
- ▶ Accompagnée d'une analyse de la valeur, incluant notamment les impacts fonctionnels, techniques, financiers, organisationnels et de sécurité.

Ces propositions ne sauraient en aucun cas emporter acceptation tacite. Aucune implémentation, mise en œuvre ou engagement de travaux relatifs à ces propositions ne pourra être réalisé sans validation préalable, formelle et écrite des divisions compétentes de l'AFD, selon les processus de gouvernance en vigueur.

À défaut de validation expresse, le TITULAIRE demeure tenu de se conformer strictement au Cadre de Référence et à ses compléments.

La présente annexe :

- ▶ N'a pas vocation à constituer une documentation exhaustive du SI existant ;
- ▶ Ne saurait engager l'AFD sur des choix techniques ou des trajectoires d'évolution non explicitement formalisés dans les documents contractuels ;
- ▶ Ne limite pas la capacité du TITULAIRE à proposer des solutions innovantes, sous réserve du respect du cadre et des principes exposés.
- ▶ Complète le cadre technique joint au dossier, intitulé : « Annexe 7 – AFD – DSI – Cadre de Référence Technique ».

Le TITULAIRE est invité à prendre en compte l'ensemble des contraintes décrites dans cette annexe dans leurs propositions, et à signaler toute incompatibilité ou point de vigilance identifié. Dans un souci de protection des informations sensibles, le présent document :

- ▶ Ne décrit pas les architectures techniques détaillées ;

- ▶ Ne présente pas les flux applicatifs, leurs volumétries ou leurs protocoles ;
- ▶ Ne communique pas d'informations sur les topologies réseau, les zones de sécurité ou les configurations internes ;
- ▶ Ne précise pas les technologies, versions ou dimensionnements.

Les éléments détaillés nécessaires à la mise en œuvre seront communiqués ultérieurement dans un cadre sécurisé au titulaire retenu.

Présentation générale du système d'information

1.1. Rôle du système d'information

Le système d'information (SI) de l'AFD constitue un levier central de soutien aux missions de l'établissement. Il permet de porter les processus métiers, de sécuriser les opérations, de garantir la traçabilité et de fournir les capacités nécessaires au pilotage, à la conformité réglementaire et à la continuité des activités.

Le SI est conçu comme un socle transverse, au service :

- ▶ Des activités opérationnelles et financières ;
- ▶ Des fonctions de pilotage, de contrôle et de reporting ;
- ▶ Des fonctions de support (ressources humaines, gestion administrative, etc.).

1.2. Périmètre fonctionnel couvert

Le système d'information couvre un large périmètre fonctionnel, correspondant aux principaux domaines d'activité de l'AFD.

À titre indicatif, il supporte notamment :

- ▶ La gestion des projets, programmes et concours ;
- ▶ Les opérations financières et la gestion du bilan ;
- ▶ La gestion de fonds pour compte de tiers et de fonds de garantie ;
- ▶ Les fonctions comptables et financières ;
- ▶ La gestion des ressources humaines ;
- ▶ Les fonctions de pilotage, de reporting et de contrôle.

Ce périmètre s'appuie sur un ensemble d'applications métiers, de progiciels du marché et de services transverses, organisés selon des principes d'urbanisation et de mutualisation.

1.3. Enjeux structurants du SI

- ▶ Conformité réglementaire : Le SI doit répondre à des exigences réglementaires et normatives fortes, notamment en matière de traçabilité, de contrôle et de protection des données.
- ▶ Interopérabilité et évolutivité : Le SI est appelé à évoluer dans le temps. Les solutions doivent s'inscrire dans une logique d'intégration maîtrisée et d'évolutivité.

Internationalisation et multi-sites : Le SI supporte des utilisateurs et des entités répartis sur plusieurs sites, en France et à l'international, avec des contraintes de connectivité et d'usage variées.

2. Gouvernance du système d'information et principes directeurs

2.1. Principes généraux de gouvernance du SI

Le système d'information de l'AFD est piloté dans le cadre d'une gouvernance structurée, visant à garantir :

- ▶ L'alignement du SI avec les objectifs stratégiques de l'établissement ;
- ▶ La maîtrise des risques, des coûts et des délais ;
- ▶ La cohérence globale des choix fonctionnels, applicatifs et techniques ;
- ▶ Le respect des exigences de sécurité.

Cette gouvernance s'inscrit dans une logique de responsabilisation partagée entre les métiers et la DSI.

2.2. Organisation générale de la gouvernance

La gouvernance du SI repose notamment sur :

- ▶ Une direction des systèmes d'information (DSI) en charge de la définition, de la mise en œuvre et du maintien du cadre SI ;
- ▶ Des instances de décision et de validation permettant d'arbitrer les choix structurants ;
- ▶ Des processus formalisés couvrant les phases de spécification, de conception, de réalisation, de mise en production et d'exploitation.

Les modalités détaillées d'organisation interne et de fonctionnement des instances ne sont pas décrites dans la présente annexe.

2.3. Principes directeurs d'urbanisation du SI

L'AFD s'appuie sur des principes d'urbanisation visant à structurer durablement le SI et à en maîtriser la complexité.

Ces principes incluent notamment :

- ▶ La clarification des périmètres fonctionnels et applicatifs ;
- ▶ La limitation des redondances et des recouvrements fonctionnels ;
- ▶ La cohérence entre les domaines métiers, les applications et les données ;
- ▶ L'inscription des solutions dans une trajectoire d'évolution maîtrisée ;
- ▶ La cartographie des blocs fonctionnels et applicatifs.

Le SI privilégie la mutualisation des services transverses et la réutilisation des composants existants, afin de :

- ▶ Renforcer la cohérence globale ;
- ▶ Améliorer le niveau de sécurité ;
- ▶ Réduire les coûts d'exploitation et de maintenance ;
- ▶ Accélérer les projets.

La sécurité du SI constitue des axes structurants de la gouvernance. Les projets et solutions font l'objet d'une prise en compte des exigences de sécurité dès les phases amont. Les choix techniques et organisationnels sont évalués au regard des risques associés. Les solutions proposées doivent être conformes aux politiques et exigences de sécurité applicables.

Les évolutions du système d'information sont encadrées par des processus visant à :

- ▶ Garantir la stabilité et la qualité de service ;
- ▶ Maîtriser les impacts fonctionnels et techniques ;
- ▶ Assurer la traçabilité des décisions et des changements.

Les principes et standards d'urbanisation et d'architecture sont documentés et publiés sur l'intranet de la DSI. Les solutions proposées par le TITULAIRE devront s'inscrire dans le cadre d'urbanisation et de sécurité. Il est invité à s'appuyer, lorsque cela est pertinent, sur les socles et services mutualisés mis à disposition par l'AFD, plutôt que de proposer des solutions isolées.

2.4. Méthodes projets et modes de conduite des projets SI

Les projets SI de l'AFD sont conduits selon des méthodes formalisées, adaptées :

- ▶ A la nature du projet ;
- ▶ A son niveau de complexité et de criticité ;
- ▶ Aux contraintes techniques, de sécurité et de pilotage.

L'AFD dispose d'une méthode historique projet structurée de type cycle en V (MAPI). Cette méthode repose sur des jalons formalisés permettant de valider les choix fonctionnels, techniques et de sécurité. L'AFD met également en œuvre des méthodes agiles, lorsque le contexte du projet le permet. Ces approches restent encadrées par les exigences de gouvernance, de sécurité, d'architecture et d'exploitation de l'AFD.

Le choix du mode de conduite (cycle en V, agile ou approche hybride) est effectué par l'AFD en fonction :

- ▶ Du contexte du projet ;
- ▶ Des enjeux métiers et techniques ;
- ▶ Des exigences de sécurité et de conformité.

Des approches hybrides peuvent être mises en œuvre, combinant :

- ▶ Un cadrage et des validations structurantes en amont ;
- ▶ Une exécution itérative sur certaines phases du projet.

3. Architecture globale du système d'information (vue macro)

3.1. Principes structurants d'architecture

L'architecture du SI de l'AFD repose sur les principes directeurs suivants :

- ▶ Cohérence et urbanisation du SI : Les composants applicatifs et techniques sont organisés de manière à garantir la cohérence d'ensemble du SI et à maîtriser sa complexité ;
- ▶ Découplage et interopérabilité : Les solutions doivent limiter les dépendances fortes entre composants et favoriser des mécanismes d'intégration maîtrisés ;
- ▶ Mutualisation des capacités transverses : Les services communs (sécurité, identité, intégration, exploitation) sont mutualisés autant que possible afin d'optimiser les coûts et le niveau de service ;
- ▶ Sécurité et conformité intégrées : Les exigences de sécurité et de conformité sont prises en compte dès la conception des architectures ;
- ▶ Évolutivité et pérennité : L'architecture vise à faciliter les évolutions fonctionnelles et techniques, ainsi que la réversibilité des solutions.

3.2. Découpage macro du système d'information

À un niveau macro, le système d'information peut être appréhendé selon les grands blocs suivants :

Canaux et interfaces utilisateurs

Ce bloc regroupe les points d'accès au SI (applications métiers, portails, outils internes), ainsi que les mécanismes de gestion des sessions et des accès utilisateurs, en cohérence avec les principes d'IAM et de SSO.

Applications métiers et progiciels

Ce bloc couvre les applications supportant les activités cœur de métier et de support de l'AFD, qu'il s'agisse de solutions spécifiques, de progiciels du marché ou de services externalisés.

Données, référentiels et pilotage

Ce bloc regroupe les données opérationnelles, les référentiels partagés et les capacités de reporting et de pilotage. La gestion de la donnée s'inscrit dans un cadre de gouvernance, de qualité et de conformité.

Services transverses mutualisés

Ce bloc comprend les services techniques communs au SI, tels que :

- ▶ La gestion des identités et des accès ;
- ▶ Les mécanismes d'intégration et d'échange ;
- ▶ Les services de sécurité transverses ;
- ▶ La supervision, la journalisation et l'ordonnancement.

Ces services constituent des points d'appui privilégiés pour les projets.

Infrastructures et exploitation

Ce bloc regroupe les capacités d'hébergement, de réseau, de stockage, de résilience et d'exploitation, mises au service des environnements applicatifs.

4. Interopérabilité et intégration applicative

4.1. Principes généraux d'interopérabilité

L'interopérabilité du SI repose sur les principes suivants :

- ▶ Découplage applicatif : Les applications doivent limiter les dépendances directes entre elles et privilégier des mécanismes d'échange maîtrisés.
- ▶ Standardisation des échanges : Les échanges applicatifs s'appuient sur des standards et formats pérennes, afin de faciliter l'intégration, l'évolution et la réversibilité.
- ▶ Maîtrise des flux : Les flux applicatifs doivent être identifiés, tracés et contrôlés, dans une logique de sécurité et de gouvernance.
- ▶ Robustesse et résilience : Les mécanismes d'intégration doivent permettre de limiter l'impact des incidents et de garantir la continuité des traitements.

4.2. Cadre général d'intégration applicative

Les échanges entre applications du SI s'inscrivent dans un cadre d'intégration mutualisé, mis en place et piloté par la DSI. Les solutions proposées devront s'intégrer dans cet écosystème existant (ESB, ETL, Kafka). Les intégrations spécifiques ou point à point doivent rester exceptionnelles et dûment justifiées. Les projets doivent privilégier les mécanismes d'intégration existants plutôt que la création de dispositifs dédiés.

4.3. Typologie des échanges applicatifs

Les solutions proposées devront être capables de supporter, selon les besoins fonctionnels :

- ▶ Des échanges synchrones, pour les usages nécessitant une réponse immédiate ;
- ▶ Des échanges asynchrones, pour les traitements différés ou les flux à fort volume ;
- ▶ Des échanges événementiels, lorsque cela est pertinent.

Les prestataires sont invités à décrire, à un niveau conceptuel :

- ▶ Des types d'échanges nécessaires à leur solution ;
- ▶ Les dépendances applicatives associées ;
- ▶ Les contraintes particulières en matière de performance ou de volumétrie, sans fournir d'éléments sensibles.

4.4. Gestion des erreurs, supervision et traçabilité

Les solutions proposées devront intégrer des mécanismes permettant :

- ▶ La détection et la gestion des erreurs d'échange ;
- ▶ La reprise sur incident sans perte de données lorsque cela est requis ;
- ▶ La supervision des flux et la production d'éléments de traçabilité exploitables.

Ces mécanismes doivent faciliter les activités d'exploitation, de support et d'audit.

5. Gestion des données

5.1. Principes généraux de gestion des données

Les données constituent un actif stratégique pour l'AFD. Leur gestion repose sur les principes suivants :

- ▶ Responsabilité et maîtrise de la donnée : Chaque donnée est rattachée à un domaine fonctionnel et à une application responsable de sa création et de sa mise à jour.
- ▶ Qualité et fiabilité : Les solutions doivent contribuer à la cohérence, à l'exactitude et à la fiabilité des données utilisées.
- ▶ Sécurité et confidentialité : Les données doivent être protégées contre tout accès, usage ou divulgation non autorisés.
- ▶ Traçabilité et Auditabilité : Les accès, modifications et échanges de données doivent pouvoir être tracés à des fins de contrôle et d'audit.

5.2. Gouvernance et responsabilité sur la donnée

La gestion des données s'inscrit dans un cadre de gouvernance transverse, associant les métiers et la DSI. Chaque application est responsable des données qu'elle produit ou administre. Les prestataires devront identifier clairement les données créées, consommées ou transformées par leurs solutions. Les règles de conservation, d'archivage et de suppression des données devront être respectées. Les modalités opérationnelles de gouvernance de la donnée sont définies par l'AFD et ne sont pas détaillées dans la présente annexe.

6. Hébergement et infrastructures

6.1. Principes généraux d'hébergement

Le SI de l'AFD repose sur une architecture d'hébergement maîtrisée, conçue pour répondre aux exigences de :

- ▶ Disponibilité et continuité de service ;
- ▶ Sécurité et protection des données ;
- ▶ Conformité réglementaire ;
- ▶ Evolutivité et pérennité des solutions.

Selon la nature des applications et des services, différents modèles d'hébergement peuvent être retenus (interne, externalisé, opéré par des tiers, ou en mode SaaS), sous réserve de leur conformité au cadre défini par l'AFD.

Le SI on-premise est hébergé au sein d'un data center situé en France, opéré par un prestataire reconnu du marché. L'exploitation des infrastructures et des services est assurée en propre par les équipes de la DSI de l'AFD, selon des processus internes de supervision, d'exploitation et de sécurité. Des infrastructures de proximité sont également déployées sur certains sites utilisateurs afin de répondre à des besoins locaux spécifiques (continuité d'activité, performance, usages métiers). Par ailleurs, un site distinct héberge les capacités nécessaires à la reprise d'activité en cas d'indisponibilité majeure du site principal, conformément aux exigences de résilience de l'AFD.

6.2. Environnements et séparation des usages

Les infrastructures du SI sont organisées selon une séparation stricte des environnements, distinguant notamment :

- ▶ Les environnements de développement ;
- ▶ Les environnements d'intégration et de recette ;
- ▶ Les environnements de pré-production et de production.

Cette séparation vise à garantir la sécurité, la qualité des mises en production et la maîtrise des risques. Les solutions proposées devront être compatibles avec cette organisation et permettre une gestion différenciée selon les environnements. Le nombre d'environnements et les responsabilités du prestataire sont précisées dans la politique DSI de gestion des environnements qui ne figure pas dans cette annexe.

6.3. Environnement de travail des utilisateurs

L'AFD met à disposition de ses collaborateurs un environnement de travail standardisé, comprenant :

- ▶ Des postes de travail portables basés sur un socle système homogène,
- ▶ Des outils de productivité individuelle,
- ▶ Des solutions de collaboration et de communication,
- ▶ Des services de mobilité accessibles depuis des terminaux mobiles,
- ▶ Une solution de nomadisme sécurisé permettant l'accès aux ressources du SI à distance.

Les modalités exactes d'accès, les politiques de sécurité associées et les solutions techniques sous-jacentes sont définies et administrées par la DSI.

6.4. Mutualisation et standardisation des infrastructures

Le SI privilégie la mutualisation des ressources d'infrastructure et l'usage de standards techniques, afin de :

- ▶ Faciliter l'exploitation et la maintenance ;
- ▶ Renforcer le niveau de sécurité global ;
- ▶ Maîtriser les coûts sur le long terme.

L'architecture repose sur des infrastructures mutualisées, comprenant notamment :

- ▶ Un socle réseau centralisé (interconnexion des environnements, accès externes et distants) ;
- ▶ Des plateformes de virtualisation ;
- ▶ Des capacités de stockage centralisées.

- Des services transverses nécessaires au bon fonctionnement du SI.

Les prestataires sont invités à proposer des solutions compatibles avec des environnements mutualisés, et à limiter la mise en place d'infrastructures dédiées ou spécifiques non justifiées.

6.5. Accès aux infrastructures et sécurité d'hébergement

Les accès aux infrastructures et aux environnements sont strictement contrôlés. Les accès sont accordés selon des principes d'habilitation et de traçabilité. Les interventions sur les environnements sensibles sont encadrées et les prestataires doivent se conformer aux règles d'accès et de sécurité définies par l'AFD.

6.6. Exploitation, supervision et maintenabilité

Les infrastructures sont exploitées selon des processus industrialisés, couvrant notamment :

- La supervision des composants techniques ;
- La gestion des incidents et des changements ;
- La maintenance préventive et corrective.

Les solutions proposées devront être exploitables, supervisables et maintenables, et fournir les éléments nécessaires à leur intégration dans les dispositifs d'exploitation existants.

6.7. Sauvegarde et protection des données

La sauvegarde des données du système d'information repose sur une architecture outillée et différenciée selon les périmètres, visant à garantir la protection, l'intégrité et la restaurabilité des données, tout en tenant compte des contraintes d'exploitation locales.

- Les infrastructures déployées au sein des agences s'appuient sur une solution de sauvegarde en mode bloc, mise en œuvre à l'aide de l'outil Arcserve UDP, permettant une protection homogène des environnements locaux et une restauration rapide en cas d'incident.
- Les infrastructures centrales hébergées en data center sont protégées par une solution de sauvegarde et de résilience de niveau entreprise, basée sur la technologie Rubrik, offrant des mécanismes avancés de sauvegarde, de restauration et de sécurisation des données.

Les politiques de sauvegarde, de rétention, ainsi que les modalités de restauration sont définies et administrées par la DSI, conformément aux exigences internes de continuité d'activité, de sécurité et de conformité réglementaire. Les caractéristiques détaillées (fréquences, fenêtres de sauvegarde, objectifs de reprise, dimensionnement) ne sont pas communiquées dans le cadre du présent document.

7. Réseaux et connectivité

7.1. Principes généraux de connectivité

Le système d'information de l'AFD supporte des usages multi-sites et internationaux, impliquant des contraintes fortes en matière de :

- Sécurité des communications ;
- Disponibilité et résilience des accès ;
- Maîtrise des flux entrants et sortants.

Les solutions proposées par les prestataires devront être compatibles avec un environnement réseau sécurisé, segmenté et maîtrisé, sans nécessiter d'ouvertures non justifiées.

7.2. Interconnexion des sites et accès au SI

Les sites de l'AFD (sièges, directions régionales, agences) sont interconnectés au système d'information via des solutions de communication sécurisées, adaptées aux contraintes géographiques et locales. Les accès au SI sont réalisés via des réseaux sécurisés et contrôlés. Les solutions doivent être compatibles avec des environnements à latence variable et les dépendances à des connexions directes ou non sécurisées sont à proscrire.

Les agences et directions régionales sont interconnectées au système d'information via des solutions de communication sécurisées, adaptées aux contraintes géographiques et locales, notamment :

- ▶ Des accès VPN sur des réseaux privés,
- ▶ Des liaisons opérées de type MPLS pour certains périmètres,
- ▶ Des accès VPN sécurisés sur Internet lorsque cela est pertinent.

Ces dispositifs visent à garantir un niveau homogène de sécurité et de qualité de service, indépendamment de la localisation des utilisateurs.

Les modalités techniques précises d'interconnexion ne sont pas détaillées dans la présente annexe.

7.3. Accès distants et mobilité

Le SI permet des usages de mobilité et d'accès distant, dans un cadre strictement sécurisé. Les solutions proposées devront :

- ▶ Être compatibles avec des accès distants sécurisés ;
- ▶ Ne pas nécessiter d'exposition directe des composants internes ;
- ▶ Respecter les règles d'authentification, de contrôle d'accès et de traçabilité définies par l'AFD.

Les prestataires ne devront pas proposer de mécanismes d'accès distant non validés ou non maîtrisés.

7.4. Flux applicatifs et principes de communication

Les communications entre applications et composants du SI reposent sur des flux réseau strictement encadrés, en cohérence avec les principes d'architecture et de sécurité. Les flux doivent être explicitement identifiés et justifiés, les communications doivent être limitées au strict nécessaire et les échanges doivent s'appuyer sur des mécanismes sécurisés et tracés.

Les solutions proposées devront être conçues pour fonctionner dans un environnement où :

- ▶ Les flux entrants sont fortement contrôlés ;
- ▶ Les flux sortants sont maîtrisés ;
- ▶ Les communications non nécessaires sont bloquées par défaut.

7.5. Segmentation et cloisonnement réseau

Le réseau du SI est organisé selon des principes de segmentation et de cloisonnement, visant à :

- ▶ Limiter la propagation des incidents ;
- ▶ Renforcer la sécurité globale ;
- ▶ Maîtriser les communications entre environnements et domaines applicatifs.

Les solutions proposées devront être compatibles avec ces principes et ne pas supposer une connectivité réseau étendue ou implicite.

7.6. Résilience et performance des accès

Les dispositifs de connectivité sont conçus pour contribuer aux objectifs globaux de :

- ▶ Continuité de service ;
- ▶ Tolérance aux incidents ;
- ▶ Qualité de service adaptée aux usages.

Les solutions proposées devront être capables de fonctionner dans des contextes de :

- ▶ Variation de performance réseau ;
- ▶ Indisponibilités temporaires ;
- ▶ Reprise progressive des communications après incident.

8. Gestion des identités et des accès (IAM)

8.1. Principes généraux de gestion des identités

La gestion des identités repose sur les principes suivants :

- ▶ Identité unique de référence : Chaque utilisateur du SI est associé à une identité unique, utilisée pour l'ensemble de ses accès applicatifs.
- ▶ Centralisation de l'authentification : Les mécanismes d'authentification sont mutualisés et pilotés de manière centralisée.
- ▶ Principe du moindre privilège : Les droits accordés aux utilisateurs sont strictement limités à leurs besoins fonctionnels.
- ▶ Traçabilité des accès : Les accès et actions significatives doivent pouvoir être tracés à des fins de contrôle et d'audit.

8.2. Authentification et Single Sign-On

Le SI met en œuvre des mécanismes de Single Sign-On (SSO) permettant aux utilisateurs d'accéder aux applications autorisées sans multiplication des authentifications. Les solutions proposées devront être compatibles avec un dispositif SSO existant. L'authentification native des applications doit, lorsque cela est possible, être déléguée au système central d'IAM. Les usages spécifiques (comptes techniques, administration) font l'objet de règles distinctes. Les solutions de gestion des accès s'appuient sur des produits du marché reconnus, tels que ForgeRock AM, sans que les modalités techniques détaillées ne soient communiquées dans le présent document.

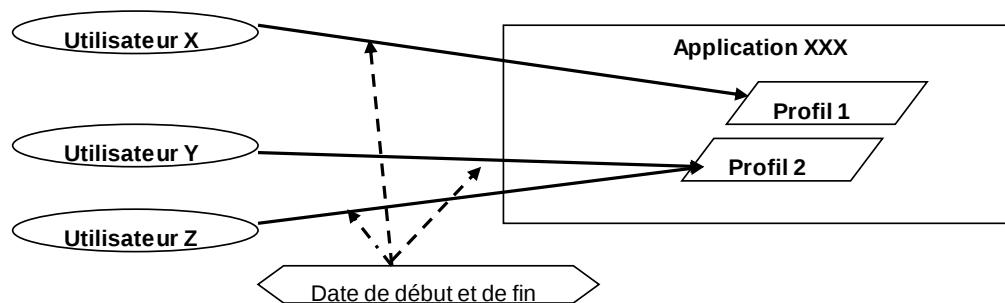
8.3. Modèle d'habilitation et gestion des droits

La gestion des habilitations repose sur un modèle structuré, fondé notamment sur :

- ▶ Des profils ou rôles d'accès applicatifs ;
- ▶ L'affectation de ces profils aux utilisateurs en fonction de leurs activités.

Les solutions proposées devront :

- ▶ Être compatibles avec ce modèle d'habilitation ;
- ▶ Éviter la multiplication de référentiels d'utilisateurs ou de droits non maîtrisés ;
- ▶ Permettre, le cas échéant, une gestion de droits fins au niveau applicatif, dérivée des profils centraux.



8.4. Intégration des applications au dispositif IAM

Toute application intégrée au SI doit pouvoir s'inscrire dans le dispositif IAM existant, selon des modes d'intégration adaptés à ses capacités techniques.

À titre indicatif, deux niveaux d'intégration peuvent être distingués :

- ▶ Un niveau d'intégration basique, permettant de bénéficier de l'authentification centralisée tout en conservant un référentiel utilisateur interne ;
- ▶ Un niveau d'intégration avancé, dans lequel l'application s'appuie sur les identités et profils transmis par le système IAM pour gérer les droits d'accès.

Les modalités techniques précises sont définies par la DSI.

8.5. Exigences techniques d'intégration (niveau conceptuel)

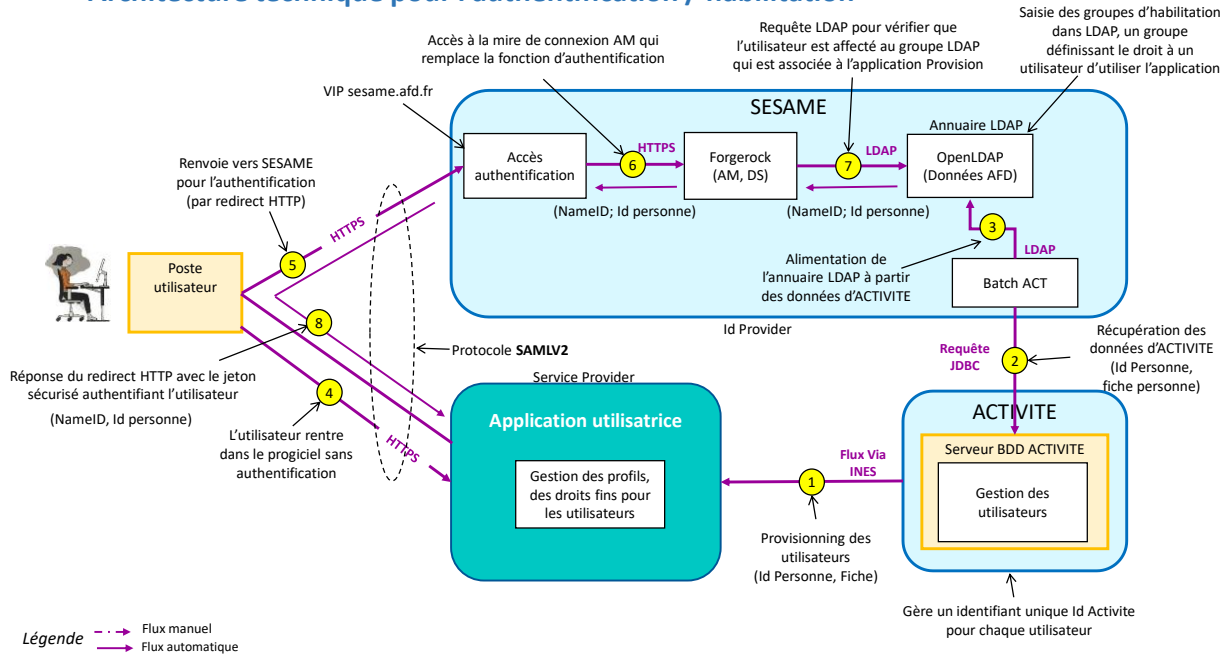
Mécanismes SSO supportés

La solution de gestion des accès met à disposition plusieurs modes d'intégration SSO standards, parmi lesquels :

- ▶ L'utilisation d'agents d'accès (web ou applicatifs) ;
- ▶ L'usage de protocoles fédérés, tels que SAML v2.

Le choix du mécanisme dépend des capacités techniques de l'application et fait l'objet d'un cadrage avec la DSI.

Architecture technique pour l'authentification / habilitation



Mode 1 – Contrôle d'accès « simple »

Ce mode permet à une application :

- ▶ De bénéficier d'une authentification centralisée via SSO ;
- ▶ Tout en conservant son référentiel interne d'utilisateurs et de droits.

Dans ce cas :

- ▶ L'infrastructure ACTIVITE assure l'authentification de l'utilisateur ;
- ▶ L'application ouvre automatiquement une session sur la base de l'identité transmise ;
- ▶ L'application reste responsable de la gestion et du stockage de ses comptes utilisateurs.

Ce mode est utilisé lorsque l'application ne peut pas s'affranchir totalement de son modèle interne de gestion des utilisateurs.

Mode 2 – Contrôle d'accès « par permissions »

Ce mode correspond à un niveau d'intégration plus avancé, dans lequel :

- ▶ L'application s'appuie sur l'infrastructure ACTIVITE pour l'authentification ;
- ▶ Les profils et attributs transmis permettent à l'application de calculer dynamiquement les droits d'accès ;
- ▶ L'application peut se passer d'un référentiel utilisateur interne.

Les informations nécessaires à la détermination des droits peuvent être mises à disposition de l'application :

- ▶ Via le contexte de la session utilisateur (ex. entêtes ou attributs de session) ;
- ▶ Ou via un accès contrôlé à un référentiel de données IAM, selon des modalités définies par la DSL.

8.6. Comptes techniques et accès privilégiés

Les comptes techniques et d'administration font l'objet d'une gestion spécifique, incluant :

- ▶ Des règles de sécurité renforcées ;
- ▶ Une traçabilité accrue des actions ;

- ▶ Une limitation stricte des usages.

Les prestataires devront intégrer ces contraintes dans la conception et l'exploitation des solutions proposées.

9. Sécurité du système d'information

9.1. Principes généraux de sécurité

La sécurité du système d'information constitue un enjeu majeur et transverse pour l'AFD. Elle est intégrée dès la conception des solutions et tout au long de leur cycle de vie, selon les principes suivants :

- ▶ Sécurité by Design et by Default : Les exigences de sécurité doivent être prises en compte dès les phases de conception et de réalisation.
- ▶ Défense en profondeur : La sécurité repose sur des mécanismes complémentaires et non sur un dispositif unique.
- ▶ Principe du moindre privilège : Les accès sont limités aux droits strictement nécessaires aux usages autorisés.
- ▶ Séparation des environnements et des responsabilités : Les environnements et les rôles sont distincts afin de limiter les risques.

9.2. Gouvernance et cadre de référence sécurité

La sécurité du SI s'inscrit dans un cadre de gouvernance formalisé, incluant :

- ▶ Des politiques et règles de sécurité internes ;
- ▶ Des processus de gestion des risques et des habilitations ;
- ▶ Des dispositifs de contrôle et d'audit.

Ce cadre s'appuie sur des référentiels reconnus, notamment ceux promus par l'ANSSI, sans que les modalités opérationnelles ne soient détaillées dans la présente annexe.

Les prestataires sont tenus de se conformer à ce cadre dans l'ensemble de leurs prestations.

9.3. Sécurité des accès et des identités

Les accès aux applications, aux données et aux infrastructures sont soumis à des mécanismes de contrôle centralisés, en cohérence avec le dispositif de gestion des identités et des accès décrit au chapitre précédent. L'authentification et l'autorisation doivent être maîtrisées et tracées. Les comptes à privilèges font l'objet de règles de sécurité renforcées et les solutions proposées ne doivent pas introduire de mécanismes d'accès non validés.

9.4. Sécurité applicative

Les solutions applicatives doivent être conçues et mises en œuvre conformément aux bonnes pratiques de sécurité applicative, notamment :

- ▶ Prévention des vulnérabilités courantes ;
- ▶ Gestion sécurisée des erreurs et des exceptions ;
- ▶ Protection contre les usages non autorisés ou malveillants ;
- ▶ Séparation des environnements applicatifs.

Les prestataires devront démontrer leur capacité à intégrer la sécurité dans leurs processus de développement, de tests et de mise en production. Si des vulnérabilités sont détectées, la mise en production peut être annulée.

9.5. Protection des données

Les solutions proposées doivent garantir un niveau de protection adapté à la sensibilité des données traitées, notamment :

- ▶ Protection contre les accès non autorisés ;
- ▶ Confidentialité et intégrité des données ;
- ▶ Traçabilité des accès et des traitements.

Les modalités détaillées de chiffrement, de classification et de journalisation des données sont définies par l'AFD et ne sont pas communiquées dans le présent document.

9.6. Journalisation, supervision et gestion des incidents

Les solutions doivent permettre :

- ▶ La journalisation des événements de sécurité pertinents ;
- ▶ Leur exploitation à des fins de supervision, d'audit et d'investigation ;
- ▶ La détection et le traitement des incidents de sécurité.

En cas d'incident de sécurité affectant le périmètre de la prestation, le prestataire est tenu :

- ▶ D'en informer l'AFD dans les délais définis contractuellement ;
- ▶ De coopérer aux actions d'analyse, de remédiation et de retour d'expérience.

9.7. Sécurité des infrastructures et de l'hébergement

Les infrastructures hébergeant les solutions doivent respecter les exigences de sécurité de l'AFD, notamment en matière :

- ▶ De contrôle des accès ;
- ▶ De segmentation et de protection des environnements ;
- ▶ De continuité et de résilience.

Lorsque l'hébergement est assuré par un tiers, le prestataire devra démontrer la conformité du dispositif proposé aux exigences de sécurité applicables.

10. Contraintes réglementaires et conformité

10.1. Cadre réglementaire général

L'AFD évolue dans un environnement institutionnel et financier fortement réglementé, impliquant des exigences accrues en matière :

- ▶ De sécurité des systèmes d'information ;
- ▶ De protection des données ;
- ▶ De traçabilité et d'auditabilité ;
- ▶ De maîtrise des risques opérationnels.

À ce titre, les solutions proposées doivent être conformes à l'ensemble des réglementations applicables et compatibles avec les dispositifs de contrôle interne de l'AFD.

10.2. Protection des données à caractère personnel

Lorsque la prestation implique le traitement de données à caractère personnel, les solutions proposées devront respecter les principes applicables en matière de protection des données, notamment :

- ▶ Licéité, loyauté et transparence des traitements ;
- ▶ Limitation des finalités et minimisation des données ;

- ▶ Intégrité, confidentialité et sécurité des données ;
- ▶ Conservation limitée dans le temps.

Les prestataires devront démontrer leur capacité à :

- ▶ Intégrer les principes de protection des données dès la conception (*Privacy by Design*) ;
- ▶ Mettre en œuvre des mesures techniques et organisationnelles appropriées ;
- ▶ Contribuer, le cas échéant, aux analyses d'impact relatives à la protection des données.

Les responsabilités respectives de l'AFD et du prestataire seront précisées contractuellement.

10.3. Sécurité du SI et gestion des risques

La conformité du SI repose sur un cadre structuré de gestion des risques liés aux systèmes d'information, couvrant les risques techniques, organisationnels et opérationnels.

Ce cadre s'appuie sur des référentiels reconnus, notamment ceux promus par l'ANSSI, ainsi que sur les exigences applicables aux établissements financiers. Les prestataires sont tenus de :

- ▶ Prendre en compte ces exigences dans la conception et la mise en œuvre des solutions ;
- ▶ Coopérer avec l'AFD dans les démarches d'analyse et de traitement des risques ;
- ▶ Signaler toute vulnérabilité ou non-conformité identifiée.

10.4. Continuité d'activité et résilience opérationnelle

Les solutions proposées doivent contribuer aux objectifs globaux de continuité d'activité et de résilience opérationnelle du système d'information. Les prestataires devront concevoir des solutions robustes face aux incidents techniques et de sécurité, documenter les dépendances critiques de leurs solutions et faciliter la mise en œuvre de mécanismes de sauvegarde et de reprise.

Les objectifs chiffrés et scénarios détaillés ne sont pas communiqués dans la présente annexe.

10.5. Traçabilité, auditabilité et contrôles

Les solutions doivent permettre un niveau de traçabilité suffisant pour répondre aux exigences :

- ▶ De contrôle interne ;
- ▶ D'audit interne et externe ;
- ▶ De supervision et d'investigation.

Les prestataires devront permettre l'accès, dans un cadre maîtrisé, aux éléments nécessaires aux contrôles réalisés par les fonctions internes de l'AFD ou par les autorités compétentes, telles que l'ACPR.

10.6. Localisation des données et recours à des tiers

Lorsque les solutions proposées reposent sur des services opérés par des tiers (hébergement externalisé, cloud ou SaaS), les prestataires devront :

- ▶ Préciser les principes de localisation et d'hébergement des données ;
- ▶ Décrire la chaîne de sous-traitance éventuelle ;
- ▶ Garantir la conformité des prestataires et sous-traitants aux exigences réglementaires applicables.

Les modalités détaillées de contractualisation et de contrôle seront précisées dans les documents contractuels.

10.7. Responsabilités et engagements des prestataires

Le prestataire est responsable :

- ▶ De la conformité réglementaire des solutions qu'il propose ;
- ▶ Du respect des obligations légales et normatives applicables à son périmètre ;
- ▶ De l'information de l'AFD en cas d'évolution réglementaire susceptible d'avoir un impact sur la prestation.

Toute non-conformité identifiée devra être signalée sans délai et faire l'objet de mesures correctives appropriées, en coordination avec l'AFD.

11. Exploitation et maintien en conditions opérationnelles,

11.1. Principes généraux d'exploitation

L'exploitation du SI repose sur des processus structurés et industrialisés, visant à :

- ▶ Assurer la continuité des services ;
- ▶ Maîtriser les incidents et les changements ;
- ▶ Garantir la sécurité et la conformité en production.

Les solutions proposées doivent être conçues pour être exploitées, dès leur conception, et s'intégrer dans les dispositifs d'exploitation existants de l'AFD.

11.2. Séparation des responsabilités Build / Run

L'AFD applique un principe de séparation entre les activités de conception/réalisation (Build) et les activités d'exploitation (Run). Les solutions doivent être livrées avec un niveau de qualité et de documentation permettant leur exploitation.

Les modalités de transfert vers les équipes en charge du Run doivent être anticipées. Les responsabilités respectives du prestataire et de l'AFD seront précisées contractuellement.

11.3. Supervision et exploitation courante

Les solutions proposées devront permettre :

- ▶ La supervision des composants applicatifs et techniques ;
- ▶ La production d'indicateurs exploitables par les équipes en charge du suivi ;
- ▶ L'intégration dans les dispositifs existants de supervision et de pilotage.

Les modalités techniques précises (outils, seuils, métriques) ne sont pas décrites dans la présente annexe.

11.4. Gestion des incidents et des anomalies

Les solutions doivent être conçues pour faciliter :

- ▶ La détection et le diagnostic des incidents ;
- ▶ La gestion des anomalies et des dysfonctionnements ;
- ▶ La mise en œuvre de correctifs dans des délais maîtrisés.

Les prestataires devront coopérer avec les équipes de l'AFD dans le cadre de la gestion des incidents, selon des modalités définies contractuellement.

11.5. Maintenance corrective et évolutive

Cette maintenance comprend :

- ▶ La maintenance corrective, visant à corriger les anomalies ;
- ▶ La maintenance évolutive, visant à accompagner les évolutions fonctionnelles ou techniques.

Les prestataires devront préciser les modalités de maintenance associées à leurs solutions, en cohérence avec les contraintes d'exploitation de l'AFD.

11.6. Gestion des changements et des mises en production

Les changements apportés au SI sont encadrés par des processus visant à :

- ▶ Limiter les impacts sur la production ;
- ▶ Garantir la traçabilité des modifications ;
- ▶ Assurer la sécurité et la conformité des mises en production.

Les solutions proposées devront être compatibles avec ces principes et faciliter les opérations de déploiement et de retour arrière si nécessaire.

11.7. Documentation et support à l'exploitation

Les solutions devront être accompagnées d'une documentation à jour et exploitable, couvrant notamment :

- ▶ L'architecture générale de la solution ;
- ▶ Les procédures d'exploitation et de support ;
- ▶ Les modalités de supervision et de diagnostic ;
- ▶ Les dépendances techniques et applicatives.

Cette documentation constitue un prérequis essentiel au bon fonctionnement du SI dans la durée. L'AFD propose des modèles pour ces documents.

12. Cycle de vie applicatif et gestion de l'obsolescence,

12.1. Principes généraux de maîtrise du cycle de vie

Le cycle de vie applicatif est piloté selon des principes visant à :

- ▶ Intégrer les contraintes d'exploitation et de sécurité dès la conception ;
- ▶ Anticiper les évolutions fonctionnelles et techniques ;
- ▶ Maîtriser les coûts et les risques sur la durée.

Les solutions proposées devront être conçues pour s'inscrire dans une trajectoire d'évolution maîtrisée, compatible avec les orientations du SI de l'AFD.

12.2. Phases du cycle de vie applicatif

Le cycle de vie d'une application couvre notamment les phases suivantes :

- ▶ Conception ;
- ▶ Réalisation et intégration ;
- ▶ Mise en production ;
- ▶ Exploitation et maintenance ;
- ▶ Evolution, remplacement ou retrait ;
- ▶ Décommissionnement.

Les prestataires devront prendre en compte l'ensemble de ces phases dans leurs propositions, y compris celles liées à la fin de vie des solutions.

12.3. Maintenabilité et évolutivité des solutions

Les solutions proposées devront être conçues de manière à :

- ▶ Faciliter la maintenance corrective et évolutive ;
- ▶ Permettre des montées de version maîtrisées ;
- ▶ Limiter les dépendances à des composants propriétaires ou en fin de support ;
- ▶ S'appuyer sur des technologies et standards reconnus et pérennes.

12.4. Gestion de l'obsolescence

L'AFD porte une attention particulière à la gestion de l'obsolescence, qu'elle soit :

- ▶ Technique (technologies, composants, infrastructures) ;
- ▶ Applicative (progiciels, frameworks, dépendances) ;
- ▶ Organisationnelle ou contractuelle.

À ce titre, les prestataires devront :

- ▶ Identifier les risques d'obsolescence associés à leur solution ;
- ▶ Proposer des mécanismes permettant d'anticiper et de traiter ces risques ;
- ▶ Informer l'AFD de toute évolution ou fin de support susceptible d'impacter la solution.

12.5. Réversibilité et fin de vie

Les prestataires devront intégrer dès la conception les principes de réversibilité et de fin de vie, notamment :

- ▶ La restitution des données dans des formats exploitables ;
- ▶ La documentation des interfaces et dépendances ;
- ▶ L'accompagnement à la transition vers une solution alternative.

Les modalités détaillées de réversibilité seront précisées contractuellement le cas échéant.

13. Attentes vis-à-vis des prestataires,

13.1. Respect du cadre SI et des principes d'architecture

Les prestataires sont attendus sur leur capacité à :

- ▶ Comprendre et respecter le cadre général du système d'information de l'AFD ;
- ▶ Concevoir des solutions compatibles avec les principes d'architecture, d'urbanisation et de mutualisation exposés ;
- ▶ S'intégrer dans l'écosystème applicatif existant sans remise en cause non justifiée.

Toute proposition s'écartant des principes décrits dans la présente annexe devra être explicitement justifiée, argumentée et soumise à validation.

13.2. Qualité des solutions et des livrables

Les prestataires devront garantir :

- ▶ Un niveau de qualité élevé des solutions proposées ;
- ▶ La conformité des livrables aux exigences fonctionnelles, techniques et de sécurité ;
- ▶ La fourniture d'une documentation claire, complète et maintenable.

Les livrables attendus devront permettre une exploitation, une maintenance et une évolution maîtrisées des solutions.

13.3. Sécurité et gestion des risques

Les prestataires sont tenus de :

- ▶ Intégrer les exigences de sécurité et de conformité dès la conception des solutions ;
- ▶ Coopérer avec les équipes de l'AFD lors des phases d'analyse de risques, de validation et de contrôle ;
- ▶ Signaler sans délai toute vulnérabilité, non-conformité ou risque identifié.

La sécurité constitue une exigence non négociable du cadre de la prestation.

13.4. Capacité d'intégration et d'exploitabilité

Les prestataires devront démontrer leur capacité à :

- ▶ Intégrer leurs solutions dans le SI existant, en cohérence avec les principes d'interopérabilité et d'IAM ;
- ▶ Concevoir des solutions exploitables, supervisables et maintenables ;
- ▶ Anticiper les contraintes du maintien en conditions opérationnelles dès la phase de conception.

Les solutions ne devront pas générer de charges d'exploitation excessives ou non maîtrisées.

13.5. Organisation, méthodes et collaboration

Les prestataires sont attendus sur :

- ▶ La clarté de leur organisation projet ;
- ▶ L'adéquation de leurs méthodes de travail avec le contexte de l'AFD ;
- ▶ Leur capacité à collaborer avec les équipes internes et les autres intervenants du SI.

La transparence, la traçabilité des décisions et la qualité de la communication constituent des éléments essentiels de la relation contractuelle.

13.6. Pérennité, évolutivité et réversibilité

Les prestataires devront démontrer :

- ▶ La pérennité des solutions proposées ;
- ▶ Leur capacité à accompagner les évolutions fonctionnelles, techniques ou réglementaires ;
- ▶ La prise en compte, dès l'amont, des principes de réversibilité et de fin de vie.

Les conditions de réversibilité feront l'objet de dispositions contractuelles spécifiques.