GROUPEMENT D'INTERET PUBLIC CARIF-OREF PROVENCE-ALPES-COTE D'AZUR

22 RUE SAINTE BARBE

13002 MARSEILLE

Ayant la forme juridique d'un Groupement d'Intérêt Public soumis aux règles de comptabilité publique applicables aux établissements publics industriels et commerciaux dotés d'un agent comptable.

Ci-après dénommé GIP Carif-Oref Provence-Alpes-Côte d'Azur

CONSULTATION - APPEL A PROPOSITIONS

Objet :

Cadre :.

Migration, mise en œuvre d'un environnement sécurisé, maintenance d'un des systèmes d'information du GIP CARIF-OREF Provence-Alpes-Côte d'Azur

Date limite de réception des offres

Le 20 janvier 2026

LE PRESENT DOCUMENT FAIT OFFICE DE DOSSIER DE CONSULTATION

Sommaire

1 — Présentation du GIP Carif-Oref Provence-Alpes-Côte d'Azur

Le GIP Carif-Oref Provence-Alpes-Côte d'Azur est un acteur régional au service de l'orientation, de la formation professionnelle et de l'emploi. Ses missions s'articulent autour de trois grands axes :

- l'observation des besoins en compétences, des évolutions des métiers et du tissu économique régional ;
- l'information et la mise à disposition de ressources fiables et actualisées auprès des professionnels de l'orientation, des organismes de formation et du grand public ;
- l'appui aux politiques publiques, par la production de données, d'études, d'outils numériques et d'analyses stratégiques.

Le GIP développe et maintient un écosystème numérique composé :

- de bases de données métiers, dont la base BROF (Banque Régionale d'Offre de Formation) ;
- d'applications en ligne (moteurs de recherche, cartographies interactives) ;
- de portails d'information ;
- de services interconnectés à des partenaires institutionnels.

Son organisation technique repose historiquement sur plusieurs prestataires spécialisés, assurant chacun une partie des services (hébergement, administration système, maintenance applicative, développement). Si ce fonctionnement a apporté de la souplesse, les évolutions des besoins et des technologies rendent désormais nécessaire une modernisation d'ensemble.

L'année 2026 marquera ainsi une phase stratégique de transition :

- modernisation de l'infrastructure numérique ;
- migration vers un hébergeur sécurisé disposant d'une infrastructure adaptée ;
- préparation de la bascule de la Banque Régionale de l'offre de Formation (BROF) vers le système mutualisé OFELI ;
- garantie de la continuité et de la performance des services, tout en maîtrisant les risques techniques.

Dans ce contexte, le présent cahier des charges vise à sélectionner un prestataire capable d'assurer :

- la migration complète de l'infrastructure externe actuelle ;
- la mise en œuvre d'un environnement sécurisé, robuste et redondant ;
- la maintenance opérationnelle du nouveau système ;la continuité de service des applications métiers et des flux techniques.

La consultation est structurée en deux lots distincts :

- **Lot 1 :** Migration de l'infrastructure externe (ECWAN, WAN, VM, DNS) ;
- **Lot 2 :** Maintenance et supervision de l'infrastructure migrée.

2 — Contexte et objectifs de la consultation

2.1 Contexte général

Le GIP Carif-Oref Provence-Alpes-Côte d'Azur dispose aujourd'hui d'une infrastructure informatique externalisée auprès de plusieurs prestataires, dont une partie critique est concernée par le présent cahier des charges. Cette infrastructure comprend notamment :

- le serveur ECWAN, qui supporte plusieurs services techniques essentiels ;
- des machines virtuelles reposant sur des systèmes Windows Server 2012 en fin de cycle de vie ;
- des bases de données et applicatifs métiers nécessitant une forte continuité de fonctionnement.

L'environnement actuel ayant atteint les limites de son cycle technologique, il devient nécessaire de le transférer vers une infrastructure d'hébergement externalisée modernisée, en reproduisant dans un premier temps l'existant afin de garantir la continuité des services. Cette migration doit également permettre d'améliorer la sécurité, les performances et la résilience, notamment par la mise en place d'une architecture redondante, idéalement répartie sur plusieurs sites.

Parallèlement, la préparation de la transition vers OFELI à partir de 2026 implique :

- le maintien de la base BROF durant la période transitoire ;
- l'adaptation progressive des applicatifs métiers qui y sont rattachés.

Les principaux points de vigilance identifiés sont :

- le besoin de renforcer significativement les ressources des futures machines (minimum 64 Go de RAM et bande passante d'au moins 2 Gbps) ;
- la mise en œuvre d'une architecture redondante ;
- la priorité accordée à la migration du WAN et des VM avant toute autre évolution.

2.2 Les quatre enjeux majeurs de la consultation

A. Continuité de service

Assurer le maintien en fonctionnement de l'ensemble des services métiers :

- bases de données ;
- moteurs de recherche ;
- interfaces d'information ;
- applications internes.

La migration devra se faire sans interruption majeure, selon un plan de bascule sécurisé.

B. Modernisation et sécurisation

Mettre en œuvre une infrastructure :

- à jour technologiquement ;
- durcie selon les bonnes pratiques de sécurité ;
- redondée et supervisée ;
- documentée pour faciliter l'exploitation et la maintenance.

C. Préparation à OFELI

La migration doit tenir compte :

- du maintien de BROF au plus tard jusqu'au 31/12/2026 ;
- du futur transfert des données vers OFELI courant 2026, au plus tard le 30/06/2026 ;

- de la nécessité de mettre à jour les applicatifs BROF en amont de la bascule nationale.

D. Rationalisation et lisibilité

Passer d'un système fragmenté entre plusieurs prestataires à une organisation plus lisible, structurée autour d'un prestataire unique pour la migration et la maintenance de l'infrastructure externalisée.

2.3 Objectifs de la consultation

L'objectif est de sélectionner un prestataire en capacité d'assurer :

Lot 1 — Migration

- le transfert intégral de l'infrastructure ECWAN vers un nouvel hébergeur ;
- la mise en place d'un environnement moderne, sécurisé et conforme aux préconisations de l'audit ;
- la gestion de la bascule du WAN et des VM ;
- la mise en service sans dégradation des performances.

Lot 2 — Maintenance

- la supervision et la maintenance opérationnelle de la nouvelle infrastructure ;
- l'administration système et réseau ;
- la gestion des incidents ;
- la garantie de continuité de service ;
- l'accompagnement du GIP lors des futures évolutions (OFELI, mise à jour des applicatifs).

3 — Périmètre de la mission

La consultation est scindée en deux lots distincts mais complémentaires :

- **Lot 1 :** Migration de l'infrastructure externe (ECWAN, WAN, VM, DNS) ;

- **Lot 2 :** Maintenance, supervision et administration de l'infrastructure migrée.

Chaque lot peut être attribué séparément. Si les lots sont attribués à deux prestataires différents, l'attributaire du Lot 1 devra assurer une transmission documentée, complète et structurée vers l'attributaire du Lot 2.

3.1 Lot 1 — Migration de l'infrastructure

3.1.1 Objectifs généraux du Lot 1

Le prestataire devra :

- migrer l'ensemble de l'infrastructure actuellement hébergée chez le prestataire en place vers un nouvel environnement sécurisé ;
- répliquer les services existants afin de garantir une mise en exploitation immédiate ;
- assurer la continuité de service et éviter toute interruption significative ;
- renforcer la sécurité, l'architecture et les performances sans modifier le fonctionnement métier ;
- fournir la documentation technique nécessaire à l'exploitation et à la maintenance futures.

3.1.2 Périmètre technique détaillé

1. Transfert du serveur ECWAN et de son architecture

Le prestataire doit assurer :

- la cartographie complète de l'existant (machines, VM, services, SQL, web, flux métiers) ;
- la reproduction de l'architecture dans le nouvel environnement (serveur dédié ou cloud IaaS) ;
- le maintien des configurations actuelles, sauf optimisation justifiée et documentée ;
- la migration des machines virtuelles ou leur reconstruction si nécessaire.

Points critiques à prendre en compte :

- machines physiques actuelles vieillissantes ;
- VM reposant sur Windows Server 2012 ;
- absence de redondance ;
- bande passante insuffisante ;
- ressources limitées nécessitant un doublement (64 Go de RAM minimum, 2 Gbps).

2. Migration du WAN et des éléments réseau

La migration inclut obligatoirement :

- le transfert du WAN actuellement géré par le prestataire en place ;
- la mise en place d'un plan de déroutement temporaire pour assurer la continuité
- la configuration du nouveau réseau externe ;
- la migration du firewall, des VPN et des règles de sécurité associées.

L'ensemble de ces opérations devra être finalisé au plus tard le **1er mars 2026**.

Il est donc demandé au prestataire de déployer une première version de l'infrastructure pour le 1er février 2026, afin d'assurer une migration progressive et des tests applicatifs sur toute la durée du mois de février.

3. Transfert et gestion du DNS

La gestion du DNS sera transférée vers un environnement cloud (OVH ou équivalent) afin de simplifier et sécuriser l'administration.

Le prestataire devra :

- migrer les zones DNS ;
- vérifier les dépendances internes et externes ;
- documenter la nouvelle configuration.

4. Sécurité & conformité

Le prestataire devra :

- renforcer la sécurité sans affecter la continuité des services ;
- mettre en œuvre les bonnes pratiques suivantes :
    - segmentation adaptée,
    - durcissement des systèmes d'exploitation,
    - journalisation centralisée,
    - gestion maîtrisée des accès administrateurs,
    - sauvegardes chiffrées et testées ;
    - proposer, le cas échéant, des améliorations de sécurité n'ayant pas d'impact majeur sur l'exploitation.

5. Plan de migration et tests

Le prestataire doit fournir :

- un plan de migration complet, validé par le CARIF-OREF ;
- un planning détaillé ;
- des tests de bascule sur l'environnement cible ;
- un procès-verbal de recette incluant :
    - la vérification des services,
    - les tests de performance,
    - le contrôle des principaux points de sécurité.

6. Documentation complète

La migration devra s'accompagner de :

- documentation technique à jour ;
- schémas d'architecture ;
- configurations (réseau, VM, firewall, DNS) ;
- procédures d'exploitation.

3.2 Lot 2 — Maintenance et supervision

3.2.1 Objectifs généraux du Lot 2

Le prestataire assurera la maintenance opérationnelle, la supervision et l'administration du nouvel environnement.

Il devra garantir :

- la disponibilité et la continuité des services ;
- la sécurité de l'infrastructure ;
- des interventions préventives et curatives adaptées ;
- une gestion structurée des incidents ;
- une documentation tenue à jour.

Le Lot 2 couvre une période initiale de **12 mois**, renouvelable par périodes de **3 mois**.

3.2.2 Périmètre technique détaillé

1. Administration système

Le prestataire prendra en charge :

- les VM Windows ou Linux ;
- la mise à jour des systèmes d'exploitation ;
- l'application des correctifs de sécurité ;
- l'administration des comptes et des accès ;
- l'optimisation des performances

2. Supervision et surveillance

Mise en place d'un système de supervision couvrant :

- charge CPU, RAM, espace disque ;
- disponibilité des services ;
- erreurs applicatives ;
- flux réseau ;
- alerting 24/7 configurable.

3. Sécurité

Le prestataire devra assurer :

- la surveillance des journaux ;
- la détection d'incidents de sécurité ;
- la gestion des failles ;
- le durcissement continu des systèmes ;
- la gestion sécurisée des sauvegardes.

4. Maintenance corrective

- diagnostic et résolution des incidents ;
- respect des délais d'intervention définis dans les SLA ;
- compte rendu systématique après chaque incident.

En cas d'incident bloquant, une intervention urgente devra être garantie.

5. Maintenance préventive

La maintenance préventive comprend notamment :

- Mises à jour régulières :
    - systèmes d'exploitation (Windows, Linux) ;
    - SQL Server ;
    - serveur web et services métiers ;
    - correctifs de sécurité critiques ;
    - firmware des hyperviseurs, le cas échéant.
- Contrôles périodiques :
    - espace disque et capacité de stockage ;
    - performances CPU/RAM ;
    - monitoring des flux réseau ;
    - vérification de l'intégrité des sauvegardes ;

- contrôle des journaux d'événements.

- Améliorations continues :
  - optimisation des performances ;
  - durcissement de la sécurité ;
  - mise à jour continue de la documentation.

6. Accompagnement « transition OFELI »

Même si le passage de la BROF à OFELI relèvera d'un marché distinct, le prestataire doit:

- garantir le bon fonctionnement de la BROF ;
- maintenir les environnements nécessaires jusqu'à la bascule ;
- accompagner les ajustements techniques liés aux phases de test et d'intégration d'OFELI.

7. Documentation et reporting

Le prestataire devra fournir :

- des comptes rendus mensuels ;
- un registre d'incidents ;
- une documentation dynamique (as-built) ;
- un suivi des principaux indicateurs (performances, disponibilités, sauvegardes, sécurité).

4 — Exigences techniques et fonctionnelles (Lot 1 : Migration)

La présente section décrit les exigences attendues du prestataire chargé de la migration de l'infrastructure externe du CARIF-OREF.

4.1 Exigences générales

Le prestataire devra respecter les principes suivants :

Continuité de service

- Aucun arrêt de service prolongé n'est acceptable.
- Une bascule progressive ou une fenêtre de maintenance planifiée devra être proposée.
- La transition devra être, autant que possible, transparente pour les utilisateurs finaux.

Reprise complète de l'existant

- Reproduction des services, configurationset règles réseau, de manière à permettre une mise en exploitation rapide, sans refonte applicative lourde.
- Modernisation de l'infrastructure
- L'architecture actuelle étant obsolète, le prestataire devra être en capacité de la moderniser et l'améliorer, tout en maintenant les service existants dans leur état actuel. Il devra donc proposer une infrastructure prenant en compte l'évolution à court et moyen terme, dans la perspective notamment de la migration vers OFELI et de la centralisation et l'homogénéisation de tous les services et applicatifs web du CARIF-OREF.

Sécurité renforcée

- Les optimisations de sécurité devront être intégrées sans impact significatif sur la disponibilité des services.
- Les recommandations issues de l'audit devront être prises en compte.

Documentation structurée

- Schémas, configurations, procédures et modes opératoires devront être remis au CARIF-OREF afin de permettre l'exploitation et, le cas échéant, la réversibilité.

Planification rigoureuse

- Le prestataire devra fournir un calendrier précis et réaliste, cohérent avec les contraintes du CARIF-OREF et les délais de migration fixés.

4.2 Exigences techniques liées à l'environnement cible

Le prestataire devra proposer une infrastructure répondant a minima aux contraintes suivantes.

4.2.1 Ressources minimales des serveurs

- 64 Go de RAM minimum, avec possibilité d'extension ;
- Processeurs dimensionnés sur la base des charges observées ;
- Stockage SSD/NVMe adapté aux besoins en I/O ;
- Capacité d'augmenter les ressources en cas de montée en charge.

4.2.2 Connectivité et bande passante

- Bande passante minimale de 2 Gbps ;
- Mise en place d'une redondance ou de mécanismes de bascule réseau.

4.2.3 Architecture technique

- Virtualisation sur un environnement moderne (Proxmox, VMware, Hyper-V nouvelle génération ou équivalent) ;
- Possibilité de déployer une architecture redondante (deux serveurs et/ou deux datacenters) ;
- Systèmes d'exploitation à jour :
    - Windows Server 2022 ou Linux, selon les besoins applicatifs ;
    - SQL Server récent ou, si nécessaire, version équivalente à l'existant dans un cadre de reproduction stricte.

- Plus généralement, tous les logiciels utilisés doivent, dans la mesure du possible, être utilisés dans leur version la plus récente possible.

4.2.4 Stratégie de sauvegarde

- Sauvegardes quotidiennes au minimum ;
- Politique de rétention adaptée à la criticité des données ;
- Stockage des sauvegardes sur un espace déporté et chiffré ;
- Test de restauration obligatoire avant mise en production.

4.3 Exigences fonctionnelles et opérations de migration

Le prestataire devra assurer l'ensemble des opérations suivantes.

4.3.1 Cartographie et audit initial

- Inventaire exhaustif des serveurs, services, VM, bases SQL, services web, scripts, tâches planifiées, ACL, flux entrants et sortants ;
- Identification des dépendances internes et externes ;
- Formulation des prérequis techniques pour la migration.

4.3.2 Mise en place de l'environnement cible

- Création et configuration de l'environnement cible ;
- Configuration d'une architecture permettant de reproduire l'intégralité des services actuellement disponibles, avec un niveau de sécurisation supérieur à l'existant, soit en reproduction à l'identique, soit en création d'une nouvelle architecture. Dans les deux cas, le candidat devra justifier les choix techniques proposés.
- Validation de la conformité de l'environnement cible avant migration effective.

4.3.3 Migration du WAN

- Reprise des paramètres réseau actuellement opérés par le prestataire en place;
- Mise en œuvre d'un plan de déroutement temporaire (switch-over) pour garantir la continuité des flux ;

- Configuration du firewall, des tunnels VPN et des règles associées.

4.3.4 Migration des machines virtuelles (VM)

- Migration à froid ou reconstruction contrôlée selon l'état et la version des systèmes (ex. Windows Server 2012) ;
- Réalisation de tests fonctionnels après migration pour chaque service concerné.

4.3.5 Migration du DNS

- Transfert des zones DNS vers OVH ou un hébergeur équivalent ;
- Vérification des dépendances applicatives et des enregistrements critiques ;
- Mise en place, le cas échéant, d'une redondance DNS.

4.3.6 Tests et vérifications

- Vérification des performances (CPU, RAM, disque, réseau) ;
- Contrôle des principaux paramètres de sécurité ;
- Validation fonctionnelle des services ;
- Recette complète en lien avec le CARIF-OREF.

4.3.7 Mise en production

- Organisation de la bascule finale ;
- Suivi renforcé pendant la période immédiatement post-migration (au minimum 7 jours ouvrés) ;
- Correction prioritaire de tout incident directement lié à la migration.

4.3.8 Transmission documentaire

Le prestataire devra fournir :

- les schémas d'architecture finale ;
- les configurations réseau et VM ;

- les règles firewall ;
- les procédures d'exploitation ;
- un inventaire complet post-migration ;
- un manuel de reprise par un tiers, en vue d'une éventuelle réversibilité.

4.4 Contraintes de planning

4.4.1 Contraintes obligatoires

- Une première implémentation doit être prête pour le 1er février 2026, avec démarrage des migrations et des tests au plus tard à cette date.
- La migration complète devra être finalisée au plus tard le 1er mars 2026 ;
- La planification devra tenir compte de la disponibilité limitée du prestataire actuel à compter de mi-janvier 2026.

4.4.2 Dépendances futures

La migration doit anticiper la transition vers OFELI, notamment :

- le maintien de BROF ;
- l'export futur des données ;
- la compatibilité des environnements.

4.5 Délais proposés

Le candidat devra fournir :

- un planning détaillé ;
- un phasage clair des étapes ;
- un projet d'infrastructure simplifié (serveurs, services, fonctionnalités…)
- une justification des choix techniques de l'infrastructure au regard des enjeux,
- les ressources mobilisées ;
- une analyse des risques et des mesures de mitigation associées.

5 — Exigences techniques et fonctionnelles (Lot 2 : Maintenance & supervision)

Le Lot 2 vise à garantir la maintenance opérationnelle, la sécurité, la supervision et la continuité de service de l'infrastructure migrée.

Il doit permettre au CARIF-OREF de disposer d'un environnement stable, sécurisé, documenté et durable.

5.1 Objectifs généraux

Le prestataire devra assurer :

La continuité des services

- garantir la disponibilité et les performances des VM, des bases SQL, des applicatifs et des services externes.

La sécurité permanente de l'infrastructure

- mettre en œuvre les mises à jour nécessaires ;
- surveiller les vulnérabilités ;
- assurer un alerting en temps réel sur les événements critiques.

Une supervision proactive

- détecter les anomalies avant qu'elles n'aient un impact sur la production.

Un niveau de service maîtrisé

- proposer des engagements clairs en matière de délais d'intervention, de traitement des incidents et de reporting.

L'accompagnement opérationnel du GIP

- soutenir le GIP dans la phase pré-OFELI et dans les évolutions futures de l'infrastructure.

5.2 Durée et modalités du marché

Durée initiale : **12 mois** ;

Marché renouvelable par périodes de **3 mois**, dans la limite fixée dans les pièces administratives.

Cette organisation permet :

- d'ajuster la durée en fonction de l'avancement du chantier OFELI ;
- d'assurer la continuité de la maintenance, y compris en cas de décalage, lorsque celui-ci résulte de contraintes inhérentes au projet ou à l'infrastructure.

5.3 Périmètre technique de la maintenance

Le prestataire devra assurer l'ensemble des aspects techniques liés à l'exploitation de l'infrastructure, incluant :

- les serveurs,
- les VM ;
- le réseau ;
- le DNS ;
- les services applicatifs ;
- les environnements SQL.

5.3.1 Maintenance corrective (incidents)

Le prestataire doit :

- diagnostiquer et corriger les incidents affectant :
    - serveurs, machines virtuelles, systèmes d'exploitation, disques, réseau, firewall, VPN, DNS ;
    - services web, SQL Server, scripts, tâches planifiées ;
    - performances ;

- intervenir dans les délais définis par les SLA (cf. section 5.6) ;
- produire un compte rendu pour chaque incident significatif.

En cas d'incident bloquant, une intervention prioritaire et rapide devra être garantie.

5.3.2 Maintenance préventive

Elle comprend notamment :

Mises à jour régulières

- systèmes d'exploitation (Windows, Linux) ;
- systèmes de base de données (SQL Server…) ;
- services webs et services applicatifs ;
- correctifs de sécurité (notamment CVE critiques) ;
- firmware des hyperviseurs, le cas échéant.

Contrôles périodiques

- espace disque et capacité de stockage ;
- performances CPU/RAM ;
- flux réseau ;
- intégrité des sauvegardes ;
- journaux d'événements

Améliorations continues

- optimisation des performances ;
- renforcement progressif de la sécurité ;
- mise à jour régulière de la documentation.

5.3.3 Supervision et alerting

Le prestataire devra déployer un dispositif de supervision couvrant :

- disponibilité des serveurs et des services ;

- charges système ;
- occupation disque ;
- erreurs applicatives ;
- disponibilité du WAN et des flux critiques ;
- surveillance DNS ;
- détection d'anomalies de sécurité.

Alerting :

- notifications en temps réel pour les incidents majeurs ;
- possibilité de notifier plusieurs interlocuteurs au sein du GIP ;
- mise à disposition d'un tableau de bord accessible au GIP (recommandé).

5.3.4 Sécurité opérationnelle

Le prestataire doit garantir :

- la gestion des accès administrateurs et des journaux ;
- la surveillance des tentatives d'intrusion ;
- le durcissement des configurations OS ;
- la mise en œuvre prioritaire des mises à jour de sécurité ;
- la gestion des sauvegardes et de leur restauration ;
- le respect du RGPD pour les traitements concernés.

Sauvegardes :

Le prestataire doit assurer :

- des sauvegardes quotidiennes au minimum ;
- une rétention adaptée à la criticité des données ;
- un stockage chiffré et déporté ;
- des tests de restauration réguliers.

5.3.5 Administration des environnements

Le prestataire doit gérer :

Systèmes d'exploitation

- Windows Server ;
- Linux (Debian, Ubuntu ou équivalent).

Bases de données

- SQL Server (notamment pour BROF) ;
- MySQL/MariaDB, si nécessaire ;
- réglages de performance, gestion des index, sauvegardes et tâches planifiées.

Réseau & sécurité

- firewall ;
- VPN ;
- VLAN et segmentation ;
- règles de routage ;
- DNS public et privé.

5.3.6 Accompagnement pré-OFELI

Même si la mise en œuvre d'OFELI fera l'objet d'un marché séparé, le prestataire devra :

- maintenir la base BROF en conditions opérationnelles jusqu'à la bascule ;
- garantir la stabilité des environnements utilisés pour l'export des données ;
- anticiper les impacts techniques liés aux phases de test et d'intégration d'OFELI.

5.4 Documentation et reporting

Le prestataire devra fournir :

Documentation technique continue

- configurations OS, SQL, firewall ;

- schémas réseaux ;
- procédures d'exploitation ;
- inventaire détaillé de l'infrastructure ;
- mise à jour régulière de ces éléments.

Reporting mensuel

- état général du système ;
- incidents traités (nature, délais, actions menées) ;
- indicateurs de performance ;
- suivi des sauvegardes (y compris tests de restauration) ;
- recommandations d'amélioration.

Registre des incidents

- mis à jour en continu ;
- consultable par le GIP.

5.5 Réversibilité / transmissibilité

En cas de changement de prestataire à l'issue du marché, le prestataire retenu devra :

- fournir une documentation complète et à jour ;
- transférer l'ensemble des accès nécessaires ;
- accompagner la reprise par le nouveau prestataire sans surcoût ;
- assurer, si besoin, une période de recouvrement.

5.6 Engagements de service (SLA)

Le candidat doit proposer des engagements sur :

Disponibilité

- Objectif minimal recommandé : 99,5 % par mois.

Délais d'intervention

- Incident critique : < 2 heures ;
- Incident majeur : < 4 heures ;
- Incident mineur : < 1 jour ouvré.

Délais de résolution

- Critique : < 8 heures ;
- Majeur : < 48 heures ;
- Mineur : < 5 jours.

Suivi et communication

- information immédiate lors d'un incident critique ;
- communication régulière jusqu'à résolution ;
- rapport de clôture pour les incidents majeurs.

5.7 Obligations du prestataire

Le prestataire devra impérativement :

- assurer la confidentialité totale des données du CARIF-OREF ;
- respecter le RGPD et les politiques de sécurité en vigueur ;
- intervenir dans le cadre strict des autorisations données ;
- mobiliser des compétences confirmées en systèmes, réseau, sécurité et SQL Server ;
- proposer un interlocuteur unique pour le GIP.

6 — Livrables attendus

Les livrables constituent les éléments que le prestataire devra remettre au CARIF-OREF au cours de la mission (Lot 1 : Migration) et tout au long de l'exploitation (Lot 2 : Maintenance).

Ils devront être fournis dans des formats ouverts (PDF, DOCX, XLSX, PNG/SVG pour les schémas) et rester la propriété exclusive du CARIF-OREF.

6.1 Livrables du Lot 1 : Migration

Le prestataire devra fournir les livrables suivants, indispensables à la mise en service de la nouvelle infrastructure.

6.1.1 Cartographie initiale de l'existant

Document comprenant notamment :

- l'inventaire des machines physiques et virtuelles ;
- les versions des OS ;
- les rôles et services associés ;
- les moteurs applicatifs, bases SQL, web, scripts ;
- les dépendances réseau (WAN, VPN, firewall, flux sortants/entrants) ;
- les schémas des communications internes et externes ;
- les points critiques identifiés.

Ce document servira de référence pour la comparaison post-migration.

6.1.2 Plan de migration détaillé

Incluant :

- un planning complet (phases, jalons, fenêtres de bascule) ;
- la méthodologie de transfert (VM, DNS, WAN, SQL) ;
- la gestion des risques et les mesures de mitigation ;
- le plan de déroutement temporaire ;
- l'analyse de l'impact prévisionnel sur les services ;

- les ressources mobilisées côté prestataire.

Ce plan devra être validé par le CARIF-OREF avant toute mise en œuvre.

6.1.3 Documentation de l'environnement cible

Le prestataire fournira une description détaillée de l'infrastructure cible :

- architecture logique et physique ;
- caractéristiques des serveurs (RAM, CPU, stockage) ;
- bande passante et mécanismes de redondance ;
- versions des OS et hyperviseurs ;
- répartition des VM ;
- paramètres serveurs SQL et serveurs web ;
- configuration DNS et firewall.

6.1.4 Procès-verbal de tests et de recette

Document présentant :

- les tests effectués avant bascule ;
- les tests fonctionnels applicatifs après migration ;
- les tests de performance (CPU, RAM, I/O, réseau) ;
- les premiers contrôles de sécurité ;
- les validations concernant le DNS, le WAN et les VM ;
- le statut de chaque service (conforme, avertissement, à corriger).

Le procès-verbal devra être signé par le CARIF-OREF et le prestataire.

6.1.5 Procédure de bascule

Le prestataire remettra :

- le déroulé détaillé de la bascule finale ;
- les conditions de retour arrière (rollback) ;
- les ressources nécessaires côté GIP ;

- les plages horaires proposées ;
- les procédures d'intervention en cas d'incident lors de la bascule.

6.1.6 Documentation post-migration

Elle devra inclure :

Documentation technique

- schémas d'architecture finale ;
- paramétrage des VM et des hyperviseurs ;
- configurations des firewalls, VPN, WAN ;
- gestion DNS (zones, TTL, redondance) ;
- configuration SQL Server ;
- paramètres serveur web et services web.

Manuel d'exploitation

- procédures standard (SOP) ;
- procédures d'urgence ;
- guide d'exploitation quotidienne ;
- politique de sauvegarde.

Manuel de reprise par un tiers

- documentation destinée à permettre la reprise de l'exploitation par un autre prestataire, notamment dans le cadre du Lot 2 ou d'un marché ultérieur.

6.1.7 Compte rendu de fin de migration

Document synthétique comprenant :

- les travaux réalisés ;
- les anomalies rencontrées ;
- les correctifs appliqués ;
- les recommandations d'amélioration ;

- les points de vigilance restant à suivre.

6.2 Livrables du Lot 2 : Maintenance

Les livrables du Lot 2 visent à assurer la lisibilité et la traçabilité de l'exploitation.

6.2.1 Tableau de bord de supervision

Le prestataire mettra en place une interface ou un rapport consolidé permettant de visualiser :

- l'état des VM ;
- la charge des ressources ;
- les alertes en cours ;
- l'historique des incidents ;
- l'état des sauvegardes ;
- la disponibilité du réseau (WAN, DNS, VPN).

6.2.2 Reporting mensuel

Chaque mois, le prestataire devra fournir un rapport incluant :

- la disponibilité des services (SLA) ;
- les incidents survenus (analyse, résolution, délais) ;
- les interventions préventives réalisées ;
- l'état des sauvegardes (dont les tests de restauration) ;
- les préconisations techniques ;
- l'état du parc de VM (performances, stockage) ;
- une synthèse des événements de sécurité (journaux, anomalies).

Le rapport devra être exploitable par le GIP sans expertise technique approfondie.

6.2.3 Registre des incidents

Document ou interface recensant pour chaque incident :

- la date et l’heure ;
- la catégorie (critique, majeur, mineur) ;
- la description ;
- les actions menées ;
- les délais d’intervention et de résolution ;
- le statut (ouvert, en cours, résolu) ;
- le responsable technique.

6.2.4 Fiches d’intervention

Pour chaque intervention significative (curative ou préventive), une fiche devra préciser :

- la nature de la tâche ;
- la durée ;
- les ressources mobilisées ;
- les impacts éventuels ;
- les résultats obtenus ;
- les recommandations associées.

6.2.5 Documentation à jour

Le prestataire devra maintenir à jour la documentation fournie dans le cadre du Lot 1 :

- schémas d’architecture ;
- paramétrages des services ;
- configurations réseau et accès ;
- procédures d’exploitation ;
- journal des mises à jour ;
- description des évolutions réalisées.

6.2.6 Réversibilité en fin de contrat

En cas de changement de prestataire, celui-ci devra remettre :

- la documentation finale complète ;
- l'ensemble des accès et secrets nécessaires, de manière sécurisée ;
- un accompagnement à la reprise par le nouveau prestataire ;
- un dossier de clôture du marché.

Aucun surcoût spécifique ne pourra être facturé au titre de la réversibilité.

7 — Modalités de réponse attendues des candidats

7.1 Plan de réponse obligatoire

Les candidats devront structurer leur réponse de la manière suivante :

Présentation du candidat

- raison sociale ;
- forme juridique ;
- historique ;
- effectifs ;
- certifications pertinentes (ISO 27001, ITIL, Microsoft, Linux, etc.) ;
- domaines d'expertise ;
- références comparables ;
- implantation géographique.

Compréhension du besoin

Le candidat devra démontrer sa compréhension :

- du contexte du GIP ;
- des contraintes de calendrier ;
- des enjeux de sécurité ;
- des attentes liées à la migration ;
- des contraintes opérationnelles en prévision d'OFELI ;
- des points critiques identifiés dans l'audit et la réunion.

Une reformulation structurée des besoins et contraintes est attendue.

Méthodologie proposée pour le Lot 1 (Migration)

Le candidat détaillera :

- sa méthodologie de migration (bonnes pratiques, outils, étapes clés) ;
- le déroulement du projet (cadrage, cartographie, préparation, tests, bascule) ;
- la gestion des risques (continuité de service, plan de retour arrière, gestion des incidents) ;
- les ressources allouées (équipe projet, chef de projet, ingénieurs systèmes/réseaux, experts SQL) ;
- le calendrier proposé, conforme aux contraintes du GIP ;
- les livrables fournis (cf. section 6.1).

Méthodologie proposée pour le Lot 2 (Maintenance)

Le candidat précisera :

- l'organisation de la maintenance (équipe dédiée, niveaux d'escalade, communication avec le GIP) ;
- la supervision et l'alerting (outils, périmètre surveillé, seuils d'alerte, reporting) ;
- la maintenance corrective (procédures, SLA, délais d'intervention) ;
- la maintenance préventive (fréquences, contrôles, mises à jour) ;
- la gestion de la sécurité (surveillance, vulnérabilités, sauvegardes, tests de restauration) ;
- les modalités de réversibilité ;
- les livrables associés (cf. section 6.2).

Architecture cible proposée

Le candidat devra présenter :

- des schémas d'architecture ;
- les ressources prévues (CPU, RAM ≥ 64 Go, stockage) ;

- la connectivité (bande passante ≥ 2 Gbps, redondance) ;
- la segmentation réseau ;
- les choix technologiques (hébergeur IaaS, hyperviseur, OS) ;
- la justification de ces choix au regard des contraintes et recommandations.

Sécurité

Le candidat détaillera :

- les mesures de durcissement ;
- la gestion des accès et des journaux ;
- la politique de sauvegarde ;
- la gestion des incidents de sécurité ;
- la conformité au RGPD ;
- les éléments de plan de reprise d'activité (PRA).

Planning

Le candidat fournira :

- un planning détaillé (Gantt ou équivalent) ;
- la description des phases, jalons et prérequis ;
- les ressources mobilisées ;
- les engagements de délai.

Conditions financières

Le candidat présentera distinctement :

- le prix du Lot 1 (migration) ;
- le prix du Lot 2 (maintenance : forfait, abonnement, etc.) ;
- les coûts des options éventuelles ;
- une grille de tarifs journaliers ou horaires, le cas échéant ;
- les conditions de paiement ;

- les éventuels frais liés aux outils.

Les prix devront être **présentés séparément** pour chaque lot.

7.2 Documents administratifs obligatoires

Le candidat devra fournir :

- les attestations fiscales et sociales ;
- un extrait Kbis de moins de 3 mois ;
- les formulaires DC1 / DC2 signés (formulaires disponibles sur le site : https://www.economie.gouv.fr/daj/formulaires-declaration-du-candidat);
- les attestations d'assurance professionnelle ;
- des références récentes (moins de 3 ans) ;
- les CV du chef de projet et des experts clés.

7.3 Format de la réponse

- Format électronique : PDF + version modifiable (Word) ;
- Respect du plan imposé ;
- Rédaction en français ;
- Mise en forme lisible, pagination ;
- Annexes clairement identifiées.

7.4 Délai et modalité d'envoi

Les réponses seront adressées par mail uniquement au plus tard le 20 janvier 2026 à :

lperrin@cariforef.fr

copie à : emaurel@cariforef.fr / mapa@cariforef.fr

Les plis et envois numériques de l'offre délivrés après la date et l'heure précitée ne seront pas retenus.

Les propositions non retenues présentées par les candidats demeurent leur propriété intellectuelle. Le contenu de ces offres sera tenu pour confidentiel, ne sera ni divulgué, ni utilisé sauf accord du candidat.

8 — Critères d'évaluation des offres

L'analyse des offres sera effectuée par le GIP Carif-Oref PACA sur la base de critères pondérés.

Chaque lot sera évalué séparément, selon les mêmes critères, afin de garantir une cohérence globale.

8.1 Critères et pondérations

1. Valeur technique de l'offre – 45 %

Appréciation de :

- la compréhension du besoin, du contexte et des contraintes ;
- la pertinence de la méthodologie proposée (migration / maintenance) ;
- la qualité de l'organisation et de la gestion de projet ;
- la cohérence entre besoins, contraintes et solutions ;
- la prise en compte de la continuité de service ;
- les mesures de sécurité ;
- les engagements en matière de supervision, de maintenance et d'intervention ;
- l'alignement avec l'audit et les échanges préalables.

2. Adéquation de l'architecture technique – 25 %

Appréciation de :

- la pertinence et la robustesse de l'architecture cible ;
- le respect des prérequis (64 Go RAM, ≥ 2 Gbps, redondance, OS à jour) ;
- la qualité des choix techniques (serveurs, hyperviseurs, OS, SQL, DNS, sauvegardes) ;
- l'évolutivité et la pérennité de l'environnement ;

- les garanties de sécurité et de durcissement ;
- la prise en compte des futures transitions (OFELI).

3. Organisation, compétences et ressources – 15 %

Appréciation de :

- l'expérience du chef de projet ;
- l'expertise des équipes systèmes/réseaux/SQL ;
- les certifications (Microsoft, Linux, ITIL, ISO 27001, etc.) ;
- la pertinence des références récentes ;
- la disponibilité des équipes ;
- la capacité à accompagner la bascule et le suivi opérationnel.

4. Prix – 15 %

Le prix sera évalué :

- lot par lot ;
- sur la base du coût global et détaillé ;
- au regard de la cohérence entre prix, charge et niveau de service.

Le prix n'est pas un critère majoritaire afin de privilégier la continuité de service et la sécurité.

5. Engagements de service (SLA) – 10 %

Appréciation de :

- les délais d'intervention et de résolution ;
- la disponibilité garantie ;
- la qualité du reporting ;
- l'organisation de la supervision ;
- les dispositifs d'astreinte, le cas échéant.

8.2 Méthode d'analyse

Pour chaque critère, une note sur 10 sera attribuée, puis pondérée selon les pourcentages ci-dessus.

Un tableau récapitulatif pourra être établi, avec une note globale sur 10 par candidat et par lot.

La meilleure note finale déterminera l'attributaire, sous réserve que l'offre soit régulière, acceptable et appropriée.

8.3 Analyse séparée des lots

- Chaque lot fera l'objet d'une analyse et d'un classement distincts ;
- Le GIP pourra retenir des prestataires différents pour chaque lot ;
- Le GIP pourra également attribuer les deux lots au même candidat si son offre est globalement la mieux classée.

8.4 Réserves du GIP

Le GIP se réserve le droit :

- de ne pas attribuer le marché si aucune offre n'est jugée satisfaisante ;
- d'engager des négociations avec un ou plusieurs candidats ;
- de solliciter des précisions ou justificatifs complémentaires ;
- de demander, le cas échéant, une démonstration ou une simulation technique.

9 — Clauses contractuelles et obligations juridiques

9.1 Nature et durée du marché

9.1.1 Type de marché

Le présent marché relève d'un appel à projet simplifié de services informatiques, passé conformément à nos procédures d'achats internes et ne peut excéder 20 000 €HT.

9.1.2 Durée du marché

- **Lot 1 (Migration)** : limité à l'exécution de la prestation, jusqu'à validation de la recette.
- **Lot 2 (Maintenance)** : durée initiale de 12 mois, renouvelable par périodes de 3 mois, selon les conditions précisées dans les pièces administratives.

9.2 Obligations générales du titulaire

Le titulaire s'engage à :

- exécuter ses obligations avec diligence, professionnalisme et impartialité ;
- mobiliser les moyens humains et techniques nécessaires ;
- garantir la continuité de service dans le périmètre défini ;
- respecter les bonnes pratiques de sécurité et de gouvernance ;
- alerter immédiatement le GIP en cas d'incident majeur ou de risque critique ;
- respecter les délais d'intervention prévus ;
- se conformer aux normes et réglementations en vigueur.

9.3 Confidentialité et protection des données

Le titulaire :

- est tenu à une obligation de confidentialité ;
- ne peut divulguer aucune information sans accord écrit du GIP ;
- doit mettre en œuvre des mesures adaptées pour protéger les données ;
- respecte le RGPD pour toutes les données concernées ;
- impose les mêmes exigences à ses sous-traitants éventuels.

9.4 Propriété intellectuelle

- Les livrables produits dans le cadre du marché deviennent la propriété exclusive du GIP ;
- Les configurations, scripts, outils et documentations créés pour le projet sont cédés au GIP avec droit d'usage complet ;

- Aucun verrou technique ne peut être mis en place sans accord explicite du GIP.

9.5 Sous-traitance

Toute sous-traitance :

- doit être demandée explicitement ;
- doit être autorisée par le GIP ;
- est soumise aux mêmes obligations (sécurité, confidentialité, réversibilité).

Le titulaire demeure responsable de l'ensemble des prestations, y compris celles réalisées par des sous-traitants.

9.6 Clauses financières

9.6.1 Modalités de facturation

- Lot 1 : facturation à l'achèvement de la prestation (avec possibilité de découpage en phases, si précisé dans l'offre) ;
- Lot 2 : facturation mensuelle ou trimestrielle selon les modalités retenues.

9.6.2 Prix fermes

Les prix sont fermes pour la durée du contrat, sauf clause de révision expressément prévue.

9.6.3 Pénalités

En cas de :

- non-respect des délais contractuels ;
- non-respect des SLA ;
- manquement grave en matière de sécurité ;
- répétition d'incidents imputables au prestataire ;

des pénalités pourront être appliquées.

9.7 Sécurité informatique

Le prestataire doit :

- respecter les bonnes pratiques de cybersécurité (ANSSI, ISO 27001, etc.) ;
- appliquer rapidement les correctifs critiques ;
- durcir régulièrement les systèmes ;
- sécuriser les accès administrateurs ;
- utiliser des connexions chiffrées (SSH, VPN) ;
- documenter les comptes et accès techniques.

En cas de faille majeure, le titulaire doit :

- informer immédiatement le GIP ;
- proposer et mettre en œuvre les mesures correctives ;
- accompagner le GIP jusqu'au retour à un niveau de sécurité satisfaisant.

9.8 Continuité de service

Le prestataire doit garantir :

- une disponibilité conforme aux SLA (cf. section 5.6) ;
- une organisation adaptée à la gestion des incidents critiques ;
- une capacité de remédiation rapide en cas de panne grave.

La continuité de service est considérée comme un objectif prioritaire du marché.

9.9 Réversibilité

En fin de contrat ou en cas de résiliation :

- le titulaire doit transférer toutes les données, configurations, accès et documentations au GIP ou au nouveau prestataire ;
- la réversibilité doit être réalisée sans surcoût ;
- le prestataire doit apporter l'assistance nécessaire à la reprise ;
- aucune dépendance technique non documentée ne doit subsister ;

- les comptes administrateurs du prestataire doivent être supprimés ou restitués selon les consignes du GIP.

9.10 Résiliation

Le marché peut être résilié, notamment :

- pour manquements répétés ;
- en cas de non-respect grave des obligations de sécurité ;
- en cas d'indisponibilités injustifiées ;
- pour abandon de projet ;
- pour motif d'intérêt général.

En cas de résiliation imputable au prestataire, les dispositions de réversibilité s'appliquent immédiatement.

9.11 Assurance

Le titulaire devra fournir :

- une attestation d'assurance responsabilité civile professionnelle ;
- le cas échéant, une couverture spécifique des risques cyber (valorisée).

9.12 Tribunal compétent

En cas de litige, le tribunal administratif compétent sera celui du ressort du siège du GIP.

10 — Annexes et documents de référence

Les documents suivants complètent le présent cahier des charges. Ils doivent être pris en compte par les candidats dans la préparation de leur offre. Toute proposition non conforme aux contraintes techniques ou calendaires issues de ces documents pourra être écartée.

10.1 Normes et référentiels applicables

Le prestataire devra se conformer aux référentiels suivants :

Sécurité informatique

- Recommandations ANSSI ;
- ISO 27001 / 27002 (bonnes pratiques) ;
- RGPD (protection des données personnelles) ;
- Bonnes pratiques de cybersécurité (CIS Benchmarks).

Informatique & Systèmes

- Bonnes pratiques ITIL (gestion des incidents, des changements, des services) ;
- Recommandations éditeurs (Windows Server, SQL Server, etc.) ;
- Bonnes pratiques des hébergeurs IaaS ;
- Règles d'interopérabilité réseau (DNS, VPN, firewall).

10.2 Modèles de documents attendus en réponse

Les candidats devront intégrer à leur réponse les modèles ou documents équivalents suivants :

- plan de migration détaillé (Lot 1) ;
- planning Gantt ;
- fiche méthodologique de maintenance (Lot 2) ;
- SLA détaillés ;
- schéma d'architecture cible ;
- modèle de reporting mensuel ;

- grille tarifaire détaillée.

10.3 Questions / réponses et additifs

Le GIP pourra, le cas échéant :

- répondre aux questions des candidats ;
- publier des additifs ou précisions au cahier des charges ;

Les candidats devront intégrer ces éventuels compléments à leur réponse finale.