CRRAE-UMOA

Caisse de Retraite par Répartition Avec Epargne de l'Union Monétaire Ouest Africaine

CAHIER DES CHARGES

ACQUISITION ET DEPLOIEMENT D'UNE SOLUTION DE SUPERVISION ET D'ADMINISTRATION DE BASE DE DONNEES

Date limite de réception des offres : **le 6 août 2026 à 12h 00mn**

SOMMAIRE

I. CONTEXTE ET OBJET

Dans le cadre de son Plan Stratégique 2025-2029, la CRRAE-UMOA a défini comme un des enjeux principaux, la « *modernisation de ses services à travers une stratégie digitale orientée Client* ». Cette dynamique de transformation oblige la maîtrise du Système d'Information, qui repose sur plusieurs applicatifs critiques notamment l'application métier et les applications support. Ces systèmes s'appuient sur un parc de bases de données hétérogènes (Oracle, PostgreSQL, SQL Server, MySQL/MariaDB, etc…), qui sont exposées à des risques opérationnels et réglementaires croissants : détection tardive des incidents, absence de traçabilité des accès, visibilité insuffisante sur les performances et les capacités, et vulnérabilités en matière de sécurité des données.

A ce titre, la mise en place d'une solution de supervision et d'administration des bases de données s'inscrit directement dans cet objectif, en permettant de disposer des outils nécessaires pour assurer une gouvernance proactive, sécurisée et conforme aux exigences réglementaires des infrastructures de données.

Le présent cahier des charges a pour objet la définition des conditions de soumission à l'appel d'offres relatif à l'acquisition et au déploiement d'une solution de supervision et d'administration des bases de données à la CRRAE-UMOA, située à la Riviera-Bonoumin.

II. PRESENTATION DE LA CRRAE-UMOA

Créée le 1er juillet 1979, la Caisse de Retraite par Répartition avec Epargne de l'Union Monétaire Ouest Africaine (CRRAE-UMOA) est un organisme public sous régional de retraite, dont le Siège est établi à Abidjan, en République de Côte d'Ivoire.

Outre ses deux (02) Adhérents Fondateurs que sont la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) et la Banque Ouest Africaine de Développement (BOAD), la CRRAE-UMOA est ouverte aux banques, établissements financiers et sociétés d'assurance de l'UEMOA, ainsi qu'aux institutions financières multinationales africaines dont le siège est situé dans l'un des Etats membres de l'Union.

La CRRAE-UMOA gère deux (02) régimes de retraite par répartition, à savoir, le Régime de Retraire par Répartition du Personnel Cadre (RRPC), le Régime de retraite Complémentaire du Personnel Non-Cadre (RCPNC), un Régime de retraite Volontaire par Capitalisation (RVC) et, pour le compte de la BCEAO, un régime de retraite spécial à prestations définies (MARR). Au titre de son action sociale, la Caisse a mis en place deux (2) Fonds Autonomes d'Assurance Maladie (FAAM-RRPC et FAAM-RCPNC) au profit des retraités et de leurs ayants droit.

Les principales missions de la CRRAE-UMOA sont les suivantes :

- assurer la pérennité et la viabilité des régimes en appliquant une gestion performante et transparente, garantissant l'équilibre financier ;
- continuer à offrir aux assurés et aux adhérents les prestations et services les plus attractifs et compétitifs du marché de la retraite en Afrique ;
- fournir aux assurés et aux adhérents, des prestations et services de premier niveau s'inscrivant dans une dynamique d'amélioration continue de la qualité de service.

III. PERIMETRE DU PROJET

La solution devra couvrir l'ensemble des SGBD ou instances en production et en test au sein du SI de la CRRAE-UMOA :

- Bases de données Oracle ;
- Bases de données PostgreSQL ;
- Bases de données Microsoft SQL Server ;
- Bases de données MySQL / MariaDB ;
- Bases NoSQL et/ou autres technologies présentes ou à venir.

Elle devra offrir une supervision et une administration unifiées depuis une console centrale unique, indépendamment de la technologie sous-jacente.

Préalablement à tout déploiement, le soumissionnaire retenu devra conduire une analyse de l'existant permettant d'inventorier et de caractériser l'ensemble des bases de données en production et en test, d'évaluer l'infrastructure d'hébergement et d'identifier les contraintes techniques spécifiques à l'environnement de la CRRAE-UMOA. Les conclusions de cette analyse feront l'objet d'un rapport validé conjointement par le prestataire et la Direction du Digital et des Systèmes d'Information (DDSI), et constitueront le socle de la validation définitive du périmètre de supervision avant tout démarrage des travaux d'installation et de paramétrage.

IV. SPECIFICATIONS FONCTIONNELLES ET TECHNIQUES DE LA SOLUTION

4.1 Description générale de la solution

La solution attendue devra couvrir l'ensemble du cycle de vie opérationnel des bases de données, en assurant de manière intégrée la supervision en temps réel, l'administration centralisée, la traçabilité complète des accès, la gestion des sauvegardes, l'optimisation des performances, le pilotage de la capacité, ainsi que la sécurité et la conformité de l'ensemble du parc de SGBD de la CRRAE-UMOA. Elle devra permettre d'atteindre les objectifs stratégiques et opérationnels ci-dessous :

- assurer la haute disponibilité et la continuité de service des bases de données critiques ;
- centraliser la surveillance de l'ensemble du parc de bases de données ;
- réduire les délais de détection et de résolution des incidents ;
- optimiser les performances des bases de données en production ;
- renforcer la sécurité et la conformité réglementaire ;
- accompagner la montée en maturité de la Direction du Digital et des Systèmes d'Information (DDSI) dans la gouvernance des données.

4.2 Caractéristiques détaillées

La solution de supervision et d'administration des bases de données devra couvrir l'ensemble des domaines fonctionnels et respecter les exigences ci-après définies. Pour chaque domaine, les exigences constituent le niveau minimal attendu de la solution proposée. Le soumissionnaire devra indiquer dans son offre technique, sous forme de tableau de conformité, la prise en charge effective de chacune de ces exigences, en précisant le cas échéant les éventuelles conditions ou limites de couverture.

4.2.1. Supervision et monitoring en temps réel

La supervision en temps réel constitue la fonction centrale de la solution attendue. Elle doit permettre à la Direction du Digital et des Systèmes d'Information (DDSI) de disposer à tout moment d'une vision complète et actualisée de l'état de l'ensemble du parc de bases de données de la CRRAE-UMOA, sans nécessiter d'intervention manuelle. Cette surveillance continue couvre la disponibilité des instances, les performances système, les situations de blocage et l'activité des sessions, et constitue le socle sur lequel reposent la détection proactive des incidents et la réactivité des équipes.

- Surveillance de la disponibilité

La solution devra assurer une vérification continue et automatisée de l'accessibilité de chaque instance supervisée, en détectant sans délai tout arrêt, redémarrage ou perte de connectivité, et en alertant immédiatement les équipes concernées afin de minimiser l'impact sur les utilisateurs et les processus métier, plus précisément :

- détection en temps réel des arrêts, redémarrages et déconnexions d'instances ;
- vérification de la connectivité réseau entre l'outil et chaque SGBD ;
- surveillance de l'état des services associés ;
- mesure du temps de réponse des connexions (latence de connexion) ;
- historisation de la disponibilité pour calcul du taux d'uptime par instance / base de données (SLA interne).

- Surveillance des performances système

La dégradation des performances des bases de données constitue l'une des premières causes d'impact sur la qualité de service perçue par les utilisateurs, souvent bien avant qu'un incident déclaré ne soit détecté. La solution devra collecter et afficher en continu les indicateurs de performance de chaque instance supervisée, en couvrant l'ensemble des dimensions techniques pertinentes afin de permettre d'identifier rapidement toute dérive et d'agir avant que la situation ne devienne critique. Ces performances sont listées ci-dessous :

- consommation CPU par instance et par processus de base de données ;
- utilisation mémoire : SGA/PGA (Oracle), shared_buffers (PostgreSQL), buffer pool (SQL Server), etc… ;
- écritures I/O disque : taux de lecture/écriture, temps d'attente, files d'attente ;
- connexions actives, en attente et bloquées ;
- taux de cache hit (efficacité du cache mémoire) ;
- activité réseau : volume de données échangées par instance.

- Surveillance des verrous et blocages

La solution devra détecter automatiquement les verrous et blocages, en identifier les sessions responsables, alerter les équipes dans les délais le cas échéant. Les fonctionnalités attendues à cet effet sont les suivantes :

- détection des deadlocks avec identification des sessions impliquées ;
- identification des sessions bloquantes et bloquées avec durée du blocage ;
- alertes sur les verrous dépassant un seuil de durée configurable ;
- historique des événements de blocage pour analyse post-incident.

➢ Surveillance des sessions et connexions actives

La solution devra offrir une visibilité complète et actualisée sur l'ensemble des connexions en cours, en permettant aux équipes d'identifier instantanément les sessions problématiques, qu'il s'agisse de sessions longues, inactives ou suspectes. Les fonctionnalités attendues sous cette section, sont indiquées ci-après :

- liste en temps réel des sessions actives : utilisateur, application, requête en cours, durée ;
- identification des sessions longues dépassant un seuil configurable ;
- détection des sessions inactives prolongées (idle sessions) ;
- possibilité de terminer une session suspecte depuis la console.

4.2.2. Administration centralisée des instances

La gestion individuelle et cloisonnée de chaque base de données par des outils natifs distincts génère une charge opérationnelle importante, la solution devra offrir une console d'administration unifiée permettant de piloter l'ensemble des instances supervisées depuis un point d'accès unique, en couvrant la gestion des utilisateurs et des droits, la manipulation des objets de base de données, la planification des tâches de maintenance et le suivi des paramètres de configuration.

➢ Gestion des utilisateurs et des droits

La solution devra permettre la gestion des comptes d'accès à la console de supervision, en offrant la possibilité de créer, modifier et désactiver les comptes des utilisateurs habilités à accéder à l'outil. Cette gestion devra s'appuyer sur une synchronisation avec l'annuaire LDAP / Active Directory de la CRRAE-UMOA pour l'authentification centralisée et l'attribution des profils d'accès. Par ailleurs, la solution devra être en mesure d'analyser les droits existants sur les instances supervisées et de détecter les comptes de bases de données inactifs ou disposant de droits excessifs, afin d'alerter les équipes pour qu'elles procèdent aux corrections nécessaires via les outils natifs des SGBD concernés. Un rapport de revue périodique des droits par instance devra être disponible à cet effet pour les activités suivantes :

- création, modification et suppression de comptes utilisateurs depuis la console ;
- synchronisation avec l'annuaire LDAP / Active Directory ;
- détection des comptes inactifs ou aux droits excessifs ;
- revue périodique des droits : rapport des utilisateurs et leurs privilèges par instance.

➢ Gestion des objets de base de données

La solution devra permettre de gérer les objets de base de données, notamment :

- navigation dans la structure : schémas, tables, vues, index, procédures, fonctions ;
- gestion des espaces de stockage : tablespaces, schémas, filegroups.

➢ Planification et suivi des tâches

La solution devra gérer la planification et le suivi des tâches et inclure les fonctionnalités ci-dessous:

- planificateur intégré : scripts SQL, scripts shell, procédures de maintenance ;
- gestion des jobs : création, modification, activation/désactivation, historique d'exécution ;
- alertes en cas d'échec ou de durée anormale d'un job ;
- gestion des fenêtres de maintenance planifiées.

4.2.3. Gestion des paramètres de configuration des bases de données

La solution devra permettre d'accéder aux paramètres de configuration des bases de données et intégrer les fonctionnalités suivantes :

- consultation des paramètres d'initialisation des instances ;
- modification des paramètres depuis la console avec validation ;
- comparaison des paramètres de configuration entre instances ;
- historisation des modifications de configuration avec horodatage et auteur

4.2.4. Gestion des sauvegardes

La solution devra permettre d'accéder aux éléments suivants relatifs à la gestion des sauvegardes :

- tableau de bord centralisé de l'état de toutes les sauvegardes effectuées (succès, échec, en cours) ;
- suivi de la dernière sauvegarde réussie par instance avec horodatage précis ;
- alertes immédiates en cas d'échec ou d'absence de sauvegarde le cas échéant ;

4.2.5. Analyse des performances et optimisation

La solution devra couvrir l'identification des requêtes lentes, l'analyse des plans d'exécution, la détection des goulets d'étranglement et la proposition de pistes d'optimisation sur la base des métriques collectées, le cas échéant, notamment :

- identification et classement des requêtes lentes (slow queries) par consommation de ressources ;
- affichage du texte complet des requêtes problématiques ;
- analyse des plans d'exécution (Explain Plan) avec visualisation graphique ;
- détection des verrous et blocages avec identification des sessions impliquées ;
- analyse des wait events pour identifier les goulets d'étranglement ;
- historisation des métriques de performance sur une période configurable (minimum 90 jours).

4.2.6. Gestion de la capacité et anticipation

La saturation de l'espace de stockage d'une base de données en production est l'un des incidents les plus prévisibles et pourtant l'un des plus fréquemment subis faute d'outillage adapté. La solution devra permettre un suivi précis et continu de la consommation des ressources de stockage par instance, tablespace et schéma, et offrir des mécanismes d'anticipation afin de donner à la DDSI le temps d'agir avant d'atteindre les seuils critiques. A ce titre, la solution devra notamment permettre :

- suivi en temps réel de l'espace disque par instance, tablespace et schéma, etc… ;
- alertes proactives de saturation à des seuils paramétrables (70%, 85%, 95%) ;
- projection de la croissance des volumes sur la base des tendances historiques ;
- estimation du délai avant saturation par instance ;
- rapports de capacité pour la planification des ressources (mensuel).

4.2.7. Tableaux de bord et reporting

La solution devra proposer des tableaux de bord personnalisables offrant une vision consolidée de l'état du parc en temps réel, ainsi qu'un ensemble de rapports périodiques automatiques permettant à la DDSI de suivre les indicateurs opérationnels, de documenter les incidents et de produire les éléments nécessaires aux audits de conformité tels que :

- Dashboard global : état de santé de l'ensemble des bases de données en temps réel :
- Dashboard par SGBD et par instance ;
- Dashboard sauvegardes : état de toutes les sauvegardes du jour ;
- Dashboard audit : accès récents, alertes de sécurité ;
- Dashboards personnalisables par profil : DBA, responsable DDSI, etc… ;
- Rapports périodiques automatiques : quotidien, hebdomadaire, mensuel ;
- Export en PDF et Excel et/ou envoi automatique par email ;
- Rapport d'audit complet : toutes les actions d'administration sur une période ;
- Rapport de conformité ISO 27001 : accès aux données sensibles, gestion des droits, incidents de sécurité.

4.2.8. Contrôle des accès à la console

La solution devra mettre en œuvre des mécanismes d'authentification et de contrôle d'accès rigoureux, conformes aux politiques de sécurité du SMSI ISO 27001 de la Caisse, afin de garantir que seules les personnes habilitées puissent accéder à la console et que leurs droits soient strictement limités à leur périmètre de responsabilité, notamment :

- authentification forte obligatoire pour accéder à la console (mot de passe complexe minimum) ;
- support de l'authentification multi-facteurs (MFA) ;
- intégration LDAP / Active Directory pour l'authentification centralisée ;
- application du principe du moindre privilège ;
- gestion des profils d'accès : lecture seule, opérateur, administrateur, super-administrateur ;
- verrouillage automatique du compte après N tentatives échouées ;
- déconnexion automatique après période d'inactivité configurable.

4.2.9. Journalisation et audit interne de la console

Toute action réalisée depuis la console d'administration doit pouvoir être retracée de manière exhaustive et inaltérable, afin de garantir la traçabilité complète des opérations effectuées sur le parc de bases de données. La solution devra notamment assurer les actions ci-dessous :

- journalisation de toutes les connexions à la console (succès et échecs) avec horodatage et IP ;
- enregistrement de chaque action administrative réalisée depuis la console : qui, quoi, quand, sur quelle instance ;
- logs inaltérables et archivés sur une durée minimale ;
- export des logs pour analyse forensique ou audit de conformité ;
- alertes sur les actions sensibles en dehors des plages horaires habituelles.

4.2.10. Chiffrement des communications

- Chiffrement TLS/SSL de toutes les communications entre agents, bases supervisées et console centrale ;
- Aucune communication en clair tolérée en production ;
- Support des certificats de l'autorité de certification interne de la CRRAE-UMOA, le cas échéant.

4.2.11. Conformité SMSI et réglementaire

- Compatibilité avec les politiques de sécurité du SMSI ISO 27001 de la CRRAE-UMOA ;
- Respect des exigences de confidentialité des données personnelles (données de cotisants et allocataires) ;
- Génération de rapports de conformité exploitables dans le cadre d'audits internes ou externes ;
- Compatibilité avec les exigences et cadre normatif UEMOA.

4.2.12. Intégrations

➢ Intégration LDAP / Active Directory

- Authentification des utilisateurs de la console via l'annuaire LDAP / Active Directory de la CRRAE-UMOA ;
- Synchronisation des groupes et des rôles depuis l'annuaire pour la gestion centralisée des habilitations.

➢ Intégration avec la solution PAM (Privileged Access Management)

La solution de supervision et d'administration de base de données doit s'intégrer nativement avec la solution PAM de la CRRAE-UMOA. Le PAM gère les comptes à privilèges (DBA, comptes de service applicatifs, comptes systèmes, etc..) et constitue le point de contrôle central des accès à haut risque. Cette intégration conditionne la capacité à démontrer la maîtrise des comptes privilégiés dans le cadre ISO 27001. La solution devra notamment assurer les fonctionnalités suivantes :

- Traçabilité renforcée de toutes les actions des comptes DBA et administrateurs système - enregistrement horodaté de chaque action avec l'identité réelle de l'opérateur ;
- Alerte immédiate sur toute connexion directe à une base de données en contournement du PAM (connexion hors coffre-fort) ;
- Récupération automatique des mots de passe des comptes supervisés depuis le coffre-fort PAM - aucun mot de passe ne doit être stocké en clair dans la configuration de l'applicatif de supervision ;

- Compatibilité avec la rotation automatique des mots de passe des comptes de service gérée par le PAM - la supervision ne doit pas être interrompue lors d'une rotation ;
- Enrichissement des enregistrements de session PAM (session recording) avec le contexte base de données : requêtes exécutées, objets modifiés, résultats obtenus ;
- Rapport conjoint Solution de supervision-PAM : liste des sessions à privilèges avec détail des actions base de données associées, exploitable pour les audits ISO 27001 ;
- Le soumissionnaire devra décrire dans son offre technique les protocoles d'intégration supportés avec les principales solutions PAM du marché (CyberArk, BeyondTrust, Wallix, Thales, etc...) ;

4.2.13. Scalabilité

La solution devra être scalable pour accompagner la croissance du SI de la CRRAE-UMOA, notamment l'intégration de nouveaux applicatifs. L'ajout de nouvelles instances supervisées devra être possible sans interruption de service. Son architecture doit permettre une évolution structurée dans le Datacenter de la Caisse.

4.2.14. Compatibilité multi-SGBD

La solution doit impérativement supporter nativement, sans développement spécifique, les SGBD suivants :

- Oracle Database (versions 11g, 12c, 19c et ultérieures) - couverture complète monitoring, audit, DDL tracking ;
- PostgreSQL (versions 12 et ultérieures) ;
- Microsoft SQL Server (versions 2016 et ultérieures) ;
- MySQL et MariaDB (versions courantes) ;
- Au moins un moteur NoSQL (MongoDB ou équivalent) ;

4.2.15. Architecture de déploiement

La solution devra reposer sur une architecture de déploiement flexible, sécurisée et adaptée aux contraintes de l'environnement technique de la CRRAE-UMOA. Elle devra notamment assurer les aspects suivants :

- Mode agentless ou agent léger selon les contraintes de sécurité de chaque serveur ;
- Architecture centralisée avec serveur de supervision et console web unique ;
- Compatibilité Linux et Windows Server ;
- Support des environnements virtualisés (VMware, Hyper-V, AVH) ;
- Support des environnements conteneurisés (Docker, Kubernetes).

4.2.16. Haute disponibilité de la plateforme

La solution devra garantir une haute disponibilité de la plateforme de supervision afin d'assurer la continuité des activités d'administration et de supervision des bases de données. Cette haute disponibilité reposera notamment sur :

- Architecture haute disponibilité de la plateforme de supervision elle-même (actif/passif ou actif/actif) ;
- Disponibilité de la console de supervision ≥ 99,5% mensuelle ;
- Documentation de la procédure de reprise en cas de défaillance de la plateforme.

V. SERVICES ATTENDUS

5.1. Mise en œuvre de la solution

Les prestations attendues dans le cadre de ce projet sont :

- Audit du périmètre des bases de données ;
- Fourniture de la solution et/ou des licences ;
- Installation, configuration et déploiement de la solution ;
- Paramétrage des tableaux de bord et des alertes ;
- Formation et transfert de compétences à l'équipe informatique de la CRRAE-UMOA (prise en main console, configuration alertes, interprétation métriques, exploitation des logs etc…).

Le soumissionnaire devra proposer une méthodologie de déploiement structurée en cinq (05) phases successives et contractuelles. Chaque phase donne lieu à un livrable formel validé conjointement par le prestataire et la DDSI avant le passage à la phase suivante. Un planning prévisionnel détaillé avec jalons, livrables et responsabilités devra être fourni avec l'offre.

5.1.1. Phase 1 : Cadrage et audit de l'existant

Cette phase constitue le point de départ obligatoire de tout le projet. Le prestataire procède à un inventaire exhaustif et documenté de l'ensemble des instances de bases de données en test et en production au sein du SI de la CRRAE-UMOA, en couvrant les technologies, les versions, les serveurs hôtes, les volumes de données et les niveaux de criticité. Il évalue également l'infrastructure d'hébergement, les contraintes réseau et les politiques de sécurité en vigueur. Les conclusions de cet audit font l'objet d'un rapport de cadrage remis à la DDSI, qui servira de socle pour la validation définitive du périmètre de supervision. Aucune installation ne peut être engagée avant validation formelle de ce rapport par la CRRAE-UMOA.

5.1.2. Phase 2 : Installation et configuration de la plateforme centrale

Le prestataire procède à l'installation du serveur de supervision et de la console d'administration dans l'environnement on-premise de la CRRAE-UMOA, conformément à l'architecture validée lors de la phase de cadrage. Cette phase comprend la configuration de la haute disponibilité de la plateforme, la sécurisation des accès à la console (authentification, intégration LDAP/Active Directory, chiffrement TLS), et l'intégration initiale avec les outils de l'écosystème DDSI (PAM). A l'issue de cette phase, la plateforme est opérationnelle et prête à recevoir les connexions aux instances de bases de données.

5.1.3. Phase 3 : Déploiement des agents et connexion aux instances

Le prestataire procède au déploiement des agents de collecte ou à la configuration des connexions agentless sur l'ensemble des instances de bases de données identifiées dans le périmètre validé. Cette phase couvre tous les SGBD du périmètre : Oracle, PostgreSQL, SQL Server, MySQL/MariaDB et bases NoSQL. Pour chaque instance connectée, le prestataire vérifie la collecte effective des métriques, la remontée des données vers la console centrale et l'absence d'impact sur les performances des bases supervisées. Un procès-verbal de connexion est établi pour chaque instance validée.

5.1.4. Phase 4 : Tests et recette

Le prestataire et la DDSI conduisent conjointement un plan de recette structuré couvrant l'ensemble des critères d'acceptance définis dans le présent cahier des charges. Des scénarios de

test sont exécutés sur chaque domaine fonctionnel : simulation d'indisponibilité d'instance, déclenchement d'alertes, vérification de la capture des connexions et des opérations DDL, génération des rapports, et mesure de l'impact sur les performances des bases supervisées. Chaque test fait l'objet d'un procès-verbal signé par les deux parties. La mise en production est conditionnée à la validation de l'ensemble des critères d'acceptance définis ci-dessous :

Critères	Conditions d'acceptance
Disponibilité	Détection et alerte d'un incident simulé dans un intervalle à définir ou en moins de 5 minutes
Audit accès	Enregistrement correct de 100% des connexions de test (réussies et échouées)
Couverture SGBD	100% des instances identifiées dans le périmètre connectées et supervisées
Reporting	Génération correcte de tous les rapports prévus avec les informations pertinentes tenant compte des exigences définies dans le présent cahier des charges.
Performance	Impact CPU sur les instances supervisées mesuré et inférieur à 2%
Sécurité	Accès à la console refusé pour tout compte non habilité, journalisation effective.

5.1.5. Phase 5 : Formation et transfert de compétences

Le prestataire assure la formation de l'ensemble des profils concernés au sein de la Direction du Digital et des Systèmes d'Information (DDSI). La formation des administrateurs DBA, administrateurs techniques, etc. couvre la prise en main de la console, la configuration et l'interprétation des alertes, l'exploitation des logs d'audit, et le diagnostic des performances. La formation des responsables DDSI porte sur l'exploitation des tableaux de bord et la lecture des rapports de conformité. L'ensemble des supports de formation sont remis à la CRRAE-UMOA à l'issue de la formation et constituent un livrable contractuel.

Les soumissionnaires devront proposer une stratégie de transfert de compétence aux équipes internes de la Caisse, qui sera mise en œuvre à l'issue des travaux du déploiement de la solution. Cette stratégie devra inclure des modules de formation à l'exploitation et à l'administration de la plate-forme.

5.2. Livraison

La livraison de la solution se fera aux frais et aux risques du soumissionnaire retenu dans les locaux de la CRRAE-UMOA à l'adresse indiquée ci-dessous :

- **Complexe Immobilier CRRAE-UMOA, Rue OBIN Atsin, Riviera-Bonoumin – Cocody Abidjan (Site principal)**

5.3. Composition et qualifications de l'équipe projet

Le soumissionnaire devra présenter dans son offre technique la composition détaillée de l'équipe affectée au projet, avec les CV nominatifs, les certifications et les références de chaque membre. La CRRAE-UMOA se réserve le droit de refuser tout remplacement de membre clé en cours de projet sans accord préalable. L'équipe doit être composée à minima d'un Chef de projet, d'un Expert Sécurité / Conformité et d'un DBA spécialiste intégration.

5.4. Dispositif d'assistance et support après mise en service

Le soumissionnaire devra prévoir l'intervention d'une ressource qualifiée, apte à assurer, après la mise en service, un accompagnement des exploitants pour la prise en main, l'administration courante de l'installation ainsi que les ajustements nécessaires des configurations.
Durant la période de garantie, le prestataire apportera son assistance à la CRRAE-UMOA en prenant en charge, à distance ou sur site, toute difficulté d'usage non expressément couverte par la documentation fournie.
En outre, le support après la mise en service intègre également les mises à jour et évolutions (Patches de sécurité inclus dans le contrat de maintenance, mises à jour de compatibilité pour les nouvelles versions de SGBD, notification préalable avant toute mise à jour impactante).

VI. CONSIDERATIONS GENERALES

Toute offre ne répondant pas explicitement aux exigences du présent document cadre sera rejetée pour non-conformité.

Aucune réclamation ne pourra être faite à la CRRAE-UMOA, quant à la justification de ses choix lors de l'adjudication.

6.1 Allotissement

Le présent appel d'offre est constitué d'un (01) seul lot.

La CRRAE-UMOA se réserve le droit de modifier la composition et les quantités de ce lot, sans que les variations n'excèdent 15 % de la composition et des quantités d'origine.

6.2 Régime des prix

Les prix des prestations devront être établis sous la forme d'une pro-forma, en francs CFA.

En vertu des dispositions de l'article 10 de l'Accord de Siège conclu le 8 mai 2008 entre le Gouvernement de la République de Côte d'Ivoire et la CRRAE-UMOA, le présent marché bénéficie du régime de l'exonération de tous les impôts, droits, taxes et prélèvements d'effet équivalent, en vigueur en Côte d'Ivoire.

En conséquence, les prix et modalités financières prévus dans le présent appel d'offres s'entendent hors taxes et hors frais de douane.

6.3 Conditions et modalités de paiement

La Caisse se libèrera des sommes dues au titre du présent marché par virement ou par chèque, sur la base d'une facture correspondant au montant exigible, accompagnée de tout document attestant de l'exécution et de la validation des prestations effectuées.

Une avance forfaitaire de démarrage d'au plus 30 % du marché global pourrait être consentie par la Caisse, sur présentation d'une garantie bancaire. Elle serait déduite du paiement à effectuer à la livraison conforme des matériaux et au fur et à mesure des décomptes de travaux présentés.

Les fournisseurs préciseront les délais de livraison et d'exécution globale des prestations. Ils seront passibles d'une pénalité de 0,5 pour mille calculée sur le montant de l'offre, par jour calendaire de retard. Le montant total des pénalités encourues est plafonné à 2,5 % du montant global du marché. Passé un délai de trente (30) jours de retard de livraison, la Caisse se réserve le droit d'annuler le marché.

6.4 Garantie

La solution doit être livrée avec les dernières versions des logicielles en date. Les soumissionnaires devront préciser dans leurs offres, la durée, les conditions et les modalités de la garantie « constructeur ». Ils devront en outre, préciser dans leurs offres le coût annuel du renouvellement du support du matériel le cas échéant.

La date de prise d'effet des garanties, des services d'appui technique et des licences d'utilisation associés à la solution livrée devra être postérieure à la date de livraison dans les locaux de la CRRAE-UMOA établie par le bordereau de livraison. Le non-respect de cette clause est un motif de rejet ou de résiliation du marché pour cause de non-conformité. La garantie couvre les vices cachés pouvant affecter le fonctionnement de la solution durant la période de référence.

Par ailleurs la CRRAE-UMOA applique une retenue de garantie égale à 5% du montant total du marché jusqu'au terme de la période d'un (01) an, à compter de la date de signature du procès-verbal de réception provisoire.

6.5 Réception

La réception sera réalisée en deux phases selon la procédure suivante :

- réception provisoire après la livraison, l'installation et la configuration de la solution et le constat du bon fonctionnement ;
- réception définitive à la fin de la période de garantie d'un (01) an, après la levée de toutes les réserves émises et la constatation du bon fonctionnement de la solution livrée, installée et configurée.

Les réceptions provisoire et définitive feront l'objet de procès-verbaux signés par les deux parties.

6.6 Connaissance des conditions du marché

En faisant acte de candidature, le soumissionnaire reconnaît :

- avoir pris connaissance de la nature du marché, des prestations qui en découlent, ainsi que des contraintes y afférentes, sur la base desquelles, il a fixé le prix global et forfaitaire ;

- engager sa responsabilité en cas de carence, erreur, ou omission portant sur les renseignements donnés à la Caisse dans le cadre de sa soumission au marché.

La production des pièces administratives actualisées est obligatoire (Registre de Commerce, attestation de régularité fiscale, attestation de la caisse de sécurité sociale, attestation de responsabilité civile entreprise). **En cas d'absence ou de non-conformité d'un de ces éléments, l'offre du soumissionnaire ne sera pas recevable.**

6.7 Présentation des offres

Les offres seront présentées en deux (02) exemplaires sous format papier et un (01) autre exemplaire sur support numérique (clé USB), rangés dans une enveloppe fermée et scellée, sur laquelle il devra être écrit, sous peine de nullité :

Au coin supérieur gauche :

"APPEL D'OFFRES POUR ACQUISITION ET DEPLOIEMENT D'UNE SOLUTION DE SUPERVISION ET D'ADMINISTRATION DES BASES DE DONNEES A LA CRRAE-UMOA A LA RIVIERA-BONOUMIN"
(A n'ouvrir qu'en commission de dépouillement)

Au centre :

Monsieur le Directeur Général de la CRRAE-UMOA
Complexe immobilier de la Riviera-Bonoumin
01 BP 2056 Abidjan 01
CÔTE D'IVOIRE

L'offre devra répondre à toutes les préoccupations exprimées dans les conditions générales, ainsi que les spécifications techniques du présent cahier des charges.

La non production de l'offre numérique sous clé USB entraine le rejet de l'offre pour non-conformité.

6.8 Contenu des offres

Chaque exemplaire de l'offre devra comporter quatre (04) parties distinctes à savoir :

- Lettre de soumission,
- Présentation du soumissionnaire,
- Offre technique,
- Offre financière.

Chaque partie devra être sous enveloppe fermée portant le titre de la partie.

- *Lettre de soumission*

Les soumissionnaires devront produire une lettre de soumission précisant tous les éléments de leurs offres qui les engagent contractuellement. Cette lettre devra donc être signée par un responsable de l'entreprise soumissionnaire.

- *Présentation du soumissionnaire*

Une présentation du soumissionnaire précisant son caractère juridique et éventuellement, le lieu de tenue de la comptabilité. Elle doit comprendre également les éléments ci-dessous :

- l'attestation datant de moins de trois (3) mois indiquant que le prestataire est en règle vis-à-vis de l'Administration Fiscale de l'État où il est établi ;

- l'attestation datant de moins de trois (3) mois indiquant que le prestataire est en règle vis-à-vis de la caisse de sécurité sociale de l'État où il est établi ;
- l'attestation d'assurance pour la responsabilité civile ;
- l'attestation d'immatriculation au Registre du Commerce du lieu de résidence ;
- les preuves de l'agrément l'éditeur de la solution.

- *Offre technique*

Les offres techniques devront être présentées conformément aux dispositions ci-après :

- les spécifications techniques et fonctionnelle de la solution conformément aux exigences définies dans le présent dossier d'appel d'offres ;
- les fiches numéros de référence de l'éditeur/constructeur de la solution ;
- la liste des références de projets similaires appuyées par les attestations de bonne exécution ou tout autre document équivalent ;
- la méthodologie de conduite de projet ;
- la présentation de l'équipe projet pressentie pour réaliser la mission, identifiant nominativement chaque profil en tenant compte de la composition et des qualifications précisée au point **5.3** ;
- les CV détaillés des membres de l'équipe faisant ressortir clairement les projets pertinents, sur les dix (10) dernières années, en lien avec l'objet du présent cahier des charges ;
- la stratégie et méthodologie de déploiement proposée ;
- le budget temps détaillé par intervenants et par phases ;
- le chronogramme détaillé réalisation ;
- le plan assurance qualité.

- *Offre financière*

Les soumissionnaires devront proposer une offre financière forfaitaire et globale en Hors taxe et Hors douane, pour l'ensemble de leurs prestations (prestations de base et prestation supplémentaires). Ils devront proposer un tableau financier, comprenant les rubriques ci-après :

- désignation détaillée (logiciels, prestations d'installation et configuration, formation, support/garantie),
- quantité,
- prix unitaire,
- prix total,
- taux de remise,
- prix total net.

Les conditions devront être détaillées en faisant ressortir les honoraires, ainsi que les frais divers. Toute prestation ou service proposé par le soumissionnaire et non chiffré, sera considéré comme inclus dans l'offre et ne donnera lieu à aucun frais supplémentaire.

N.B : Le soumissionnaire devra indiquer le délai de livraison de la solution ainsi que la durée des prestations. Par ailleurs, la présentation de l'équipe projet précisant nominativement chaque profil est obligatoire. L'absence de ces éléments constitue une non-conformité.
La couverture fonctionnelle devra être présentée sous la forme d'un tableau de conformité précisant la prise en compte des exigences du cahier des charges, accompagné d'un détail explicatif pour chacune des exigences, le cas échéant.

6.9 Critères d'évaluation des offres

- Les offres seront évaluées selon les critères suivants :
- les délais de livraison ;
- la conformité de l'offre technique aux caractéristiques minimales ;
- la pertinence de l'offre financière ;
- la présentation des offres ;
- les références du soumissionnaire et expérience sur des projets similaires

6.10 Dépôt des offres

Les offres doivent être déposées au **Secrétariat de la Direction du Capital Humain, de l'Administration et du Patrimoine (DCHAP) situé au 4ème Etage A de l'Immeuble CRRAE-UMOA à Abidjan – Riviera-Bonoumin.**

6.11 Compléments d'informations

Pour obtenir des renseignements destinés à une meilleure appréciation du présent cahier des charges, les soumissionnaires peuvent adresser leur requête par messagerie électronique à l'adresse darh@crrae.org.

Les demandes de compléments d'informations devront être formulées par écrit, huit (08) jours calendaires au plus tard, après la date de lancement de cette consultation.

Les réponses y apportées, le cas échéant, seront communiquées au soumissionnaire requérant et publiées sur le site internet de la CRRAE-UMOA, à la rubrique « Avis et communiqués ».

Par ailleurs, la CRRAE-UMOA se réserve le droit de communiquer des informations complémentaires au dossier d'appel d'offres, au plus tard, huit (08) jours calendaires avant la date de clôture du dépôt des offres.