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

CAHIER DES CHARGES

POUR LE RECRUTEMENT D'UN PRESTATAIRE CHARGE DE LA MISE EN PLACE D'UN SYSTEME DE MANAGEMENT DE LA SECURITE DE L'INFORMATION (SMSI) A LA CRRAE-UMOA

Date limite de réception des offres : Vendredi 27 février 2026

Sommaire

CRRAE-UMOA
01 BP 2056 Abidjan 01
Tél.:25 22 01 83 83

1. PRESENTATION DE LA CRRAE-UMOA

La CRRAE-UMOA est un Organisme Public International de prévoyance retraite. Elle gère deux (02) régimes de retraite par répartition, à savoir le Régime de Retraite par Répartition du Personnel Cadre (RRPC), le Régime de Retraite Complémentaire du Personnel Non Cadre (RCPNC), ainsi qu'un Régime de Retraite Volontaire par Capitalisation (RVC). Elle gère également au profit des retraités, deux (2) Fonds Autonomes d'Assurance Maladie (FAAM RRPC et FAAM RCPNC).

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.

Ses principales missions 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.

2. CONTEXTE

Dans le cadre de son plan de transformation digitale initié en 2025, la CRRAE-UMOA renforce l'usage des technologies de l'information et de la communication pour améliorer la qualité de ses services, la performance de ses processus et la satisfaction de ses assurés et partenaires.

Cette transformation expose le système d'information de la Caisse à des risques de plus en plus accrus en matière de sécurité de l'information (cyberattaques, fuites de données, indisponibilité des systèmes, non-conformité réglementaire…). Compte tenu de la sensibilité des données gérées (données personnelles, financières et sociales), la CRRAE-UMOA souhaite mettre en place un Système de Management de la Sécurité de l'Information (SMSI) conforme aux bonnes pratiques internationales, notamment la norme ISO/IEC 27001.

À cet égard, la CRRAE-UMOA envisage de recruter un cabinet spécialisé pour l'accompagner dans la conception et l'opérationnalisation de son SMSI.

Le présent cahier des charges a pour objet de définir les critères de sélection du cabinet et les conditions de soumission à l'appel d'offres pour son recrutement.

3. OBJECTIFS

L'objectif principal de cette mission sera de définir un ensemble de politiques concernant la gestion de la sécurité de l'information afin d'identifier, d'évaluer et de gérer les risques autant en termes d'infrastructures physiques que de solutions logicielles. Les critères ci-dessous en particulier devront être garantis :

CRRAE-UMOA
01 BP 2056 Abidjan 01
Tél.:25 22 01 83 83

- la confidentialité : protéger l'information des parties non concernées ;
- l'intégrité : empêcher la modification de l'information par les personnes qui n'y sont pas autorisées ;
- la disponibilité : rendre l'information disponible aux personnes autorisées à y accéder ;
- la traçabilité : garantir la traçabilité des activités ou transactions dans le système ;
- l'authentification : vérifier l'identité de chaque utilisateur, afin de permettre l'accès aux ressources uniquement par les personnes autorisées.

Pour ce faire, la Caisse souhaite :

- évaluer le niveau de maturité actuel de la sécurité de son système d'information (SI) à travers la réalisation d'un audit organisationnel et technique combinant à la fois des techniques d'entretien, d'analyse de documentation, de tests d'intrusion et d'analyses de vulnérabilité par des approches manuelles et automatisées ; Cet audit devrait inclure une analyse des risques liés à la sécurité de l'information ;
- définir des objectifs de sécurité et une politique associée à mettre en œuvre pour atteindre une situation de sécurité cible appelée à être maintenue dans la durée ;
- garantir la disponibilité des services essentiels de son système d'information, même en cas de crises ou de perturbations l'affectant ;
- mettre en place les processus, procédures et contrôles du SMSI ;
- couvrir les risques pesant sur le SI et renforcer l'organisation interne pour soutenir la démarche de sécurisation du SI ;
- sensibiliser et former les acteurs clés de la CRRAE-UMOA ;
- mettre en œuvre une démarche ISO 27001 pour la mise en place d'un SMSI et s'aligner sur les bonnes pratiques internationales.

4. PERIMETRE DU SMSI

Le périmètre du SMSI couvrira notamment :

- les infrastructures informatiques (locaux informatiques, réseaux, serveurs, postes de travail, datacenters, cloud, base de données...) ;
- les applications métiers et supports ;
- les données (assurés, cotisations, prestations, finances, RH, partenaires, etc.) ;
- la conformité réglementaire ;
- les processus critiques de la CRRAE-UMOA et la continuité d'activité ;
- les utilisateurs internes, les usagers externes et les prestataires externes.

Le périmètre définitif sera validé conjointement avec le cabinet retenu.

5. PRESTATIONS ATTENDUES

Les prestations visent à mettre en place un SMSI structuré et pérenne, adapté aux risques spécifiques liés aux activités de la CRRAE-UMOA, pour renforcer durablement la sécurité de l'information, améliorer la gouvernance des données, assurer la conformité réglementaire

(protection des données personnelles, cybersécurité, interopérabilité) et poser les bases d'une future certification ISO/IEC 27001. A cet égard, la mission sera séquencée en 2 grandes étapes :

5.1 Evaluation initiale de la sécurité de l'information

Il s'agira pour le prestaire de réaliser un audit de maturité de la sécurité de l'information couvrant les dispositifs existants, les politiques, les procédures, et les outils en s'appuyant sur les précédents rapports d'audits disponibles. De manière plus détaillée, les actions suivantes sont attendues :

- analyser et évaluer l'infrastructure physique et les liens de raccordement entre ses composantes ;
- faire l'inventaire des composants réseau (routeurs, switch, firewall...) et des liens de raccordement (câblage existant) ;
- vérifier la configuration des postes et serveurs en vue de détecter d'éventuelles brèches d'intrusion ;
- diagnostiquer et évaluer la configuration réseau ;
- tester la vulnérabilité des applications ;
- vérifier les mécanismes d'authentification et d'autorisation ;
- effectuer des tests d'intrusions internes ou externes afin de détecter d'éventuelles vulnérabilités des systèmes informatiques ;
- réaliser un inventaire des actifs de la Caisse qui devra couvrir les données, les équipements, les comptes utilisateurs, les applications, etc ;
- évaluer le système de messagerie et ses mesures de sécurité (accès aux mails, filtres, spams, reporting de détection...) ;
- évaluer les connexions Internet et les points d'accès wifi ;
- évaluer les solutions de sauvegarde ;
- évaluer les dispositifs de sécurité du matériel, des données et du réseau (la protection antivirale, pare-feu, filtrage internet...), et des contrôles d'accès.

5.2 Déploiement du SMSI et de son cadre de gouvernance

Le déploiement du SMSI devra prendre en compte les outils existants, mettre en place les rôles, les responsabilités, les comités, et produire le manuel du SMSI : les indicateurs, les politiques et les procédures ;

Cette phase consistera à :

- élaborer la PSSI et les procédures associées pour l'Institution ;
- formaliser une stratégie de cybersécurité, des objectifs de sécurité, des services de sécurité, des rôles et responsabilités, une organisation cible et des besoins en technologies à déployer ;
- mettre en place un processus d'amélioration continue dans la gestion de la sécurité conformément à la norme ISO 27001 ;

- élaborer un programme de conduite du changement associé à une stratégie de sensibilisation ;
- élaborer un programme continu pour maintenir la sensibilisation de tous les employés aux risques et aux bonnes pratiques (phishing, etc.);
- mettre en place une base de données de gestion de configuration (CMDB) ;
- formaliser une cartographie des risques liés à la sécurité de l'information ;
- accompagner les acteurs à l'adoption du SMSI, les former aux bonnes pratiques de sécurité et développer un module de formation numérique réutilisable en interne : PDF, vidéos, modules e-learning, etc.) ;
- proposer une feuille de route sur 24 mois qui prend en compte la certification ISO 27001 ; chaque recommandation de la feuille de route devra faire l'objet de termes de référence avec un chiffrage associé.

Les prestations sont réparties en un seul lot.

6. DUREE DE LA MISSION

La mission du consultant s'effectuera sur une durée allant de 04 à 06 mois.

7. QUALIFICATIONS ET REFERENCES DU PRESTATAIRE

- Être un prestataire dans le domaine de la Sécurité de l'Information, les Systèmes de Management et plus spécifiquement des SMSI conformes à la norme ISO 27001.
- Disposer des ressources humaines qualifiées pour l'audit de la sécurité SI et la mise en place de SMSI, certifiées à la norme ISO 27001 : 2022. Le cabinet devra indiquer clairement et fournir les références d'au moins un expert faisant partie de son personnel permanent et qui sera le chef de mission. Cet expert doit avoir une expérience professionnelle de plus de 10 ans, être certifié aux normes ISO 27001 et CISA et disposant d'au moins deux (03) références pour un projet similaire.
- Avoir exécuté avec satisfaction, au cours des 4 dernières années (2025, 2024, 2023, 2022) au moins deux (02) missions similaires ; fournir les attestations de bonne exécution.
- L'équipe projet doit disposer en son sein, d'une expérience spécifique en Ethical Hacking et avoir des certifications professionnelles : CISCO, Fortinet, CEH, CSA, CompTIA Security+.
- Les intervenants doivent avoir une expérience spécifique en matière de sécurité des systèmes d'information : avec une expertise en Audit de sécurité SI, Tests de Pénétration, Investigation Numérique, Elaboration de politiques de sécurité SI, Assistance à la mise en place de programmes de sécurité SI.
- Les intervenants doivent avoir une expérience spécifique en audit des infrastructures de réseaux informatiques, infrastructures systèmes et infrastructures télécom.

8. LIEU DE LA MISSION

La mission se déroulera essentiellement au siège de la CRRAE-UMOA à Abidjan (Côte d'Ivoire). Toutefois, il pourrait être envisagé l'exécution à distance des actions qui ne requièrent pas une présence in situ.

9. CONFIDENTIALITE ET SECRET PROFESSIONNEL

Le prestataire devra s'engager à observer la plus stricte confidentialité, notamment s'interdire de divulguer toute information dont il aurait pris connaissance au cours de son intervention à la CRRAE-UMOA.

Les livrables et documents soumis par le contractant et élaborés au cours de cette mission, deviennent propriété exclusive de la Caisse qui pourra les utiliser sans aucune redevance, ni restriction, ni autorisation préalable. Le contractant devra ainsi remettre à la CRRAE-UMOA tous les supports originaux ayant servi à l'exécution du projet.

10. LIVRABLES

Les livrables sont attendus en deux (02) volets :

10.1 Rapport d'audit détaillé

A l'issue de l'audit global, le cabinet devra fournir à la CRRAE-UMOA un rapport détaillé contenant :

- l'inventaire exhaustif et documenté du parc ;
- la schématisation du réseau informatique ;
- les points forts et faiblesses relevées sur la sécurité ;
- l'analyse de la normalité des salles serveurs ;
- l'analyse de l'adéquation du SI par rapport à l'organisation de l'Institution ;
- la catégorisation des risques par occurrence et impact ;
- les mesures correctives.

Les recommandations issues de cette 1ère phase devront garantir à la Caisse lorsqu'elles sont mises en œuvre, que son système d'information respecte les principes suivants énumérés dans les objectifs (la confidentialité, l'intégrité, la disponibilité, la traçabilité, l'authentification).

A cette fin, elles devront inclure :

- les actions détaillées à mettre en œuvre dans l'immédiat, pour pallier les défaillances les plus graves ;
- les actions à mettre en œuvre sur le moyen terme sur les plans :
    - Organisationnel : structures et postes à créer, opérations de sensibilisation et de formation, procédures de sécurité à instaurer
    - Technique : outils et mécanismes de sécurité, amélioration des dispositifs de sécurité existants, aménagement des salles serveurs selon les normes sécuritaires appropriées
- la proposition d'un plan d'action avec un planning des mesures de sécurité à entreprendre ;

- une estimation des moyens humains et financiers à prévoir pour réaliser ces actions.

10.2 Politique de Sécurité des Systèmes d'Information (PSSI) effective

- une PSSI, des politiques générales (annexe) et des procédures de sécurité pour l'Institution ;
- une stratégie de cybersécurité incluant des objectifs de sécurité, des services de sécurité, des rôles et responsabilités, une organisation cible et des besoins en technologies à déployer ;
- un processus d'amélioration continue dans la gestion de la sécurité conformément à la norme ISO 27001 ;
- un programme continu pour maintenir la sensibilisation de tous les employés aux risques et aux bonnes pratiques (campagnes de phishing, création de contenu de sensibilisation...) ;
- un programme de conduite du changement et une stratégie de sensibilisation durable ;
- une cartographie des risques et son plan des mesures correctives ;
- une base de données de gestion de configuration (CMDB) ;
- un Tableau de bord des indicateurs de performances ;
- un Système de Management de Sécurité de l'Information (SMSI) certifiable en l'état ou après correction des écarts identifies à l'issue de l'audit blanc réalisé.

La langue de travail est le français. De ce fait tous les livrables et documents de travail devront être rédigés en langue française.

11. CONTENU DES OFFRES

Les offres seront présentées en deux (2) exemplaires sous format papier et un (1) autre exemplaire sur support numérique (clé USB) ; le tout rangé dans une enveloppe fermée et scellée, sur laquelle il devra être écrit, sous peine d'être considérées comme nulles :

Au coin supérieur gauche :

" APPEL D'OFFRES POUR LE RECRUTEMENT D'UN PRESTATAIRE CHARGE DE LA MISE EN PLACE D'UN SYSTEME DE MANAGEMENT DE LA SECURITE DE L'INFORMATION (SMSI) A LA CRRAE-UMOA "
A n'ouvrir qu'en commission de dépouillement "

Au centre :

Monsieur le Directeur Général de la CRRAE-UMOA
Complexe Immobilier CRRAE-UMOA,
Rue OBIN Atsin, Riviera-Bonoumin,
Cocody • 01 BP 2056 Abidjan 01
CÔTE D'IVOIRE

En outre, chaque exemplaire de l'offre devra comporter quatre (04) parties distinctes à savoir :

- Lettre de soumission ;
- Présentation du soumissionnaire ;

CRRAE-UMOA
01 BP 2056 Abidjan 01
Tél.:25 22 01 83 83

- 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 ;

Offre technique

L'offre technique devra obligatoirement inclure tous les renseignements nécessaires à sa bonne évaluation, notamment :

- l'exposé de sa compréhension de la mission ;
- l'exposé de la démarche méthodologique détaillée en précisant, éventuellement, les outils méthodologiques et les normes spécifiques qu'il entend utiliser ;
- les références du prestataire dans des interventions similaires qui devront être corroborées par des attestations de bonne exécution) ;
- la composition de l'équipe d'intervenants avec les curriculums vitae nominatifs et détaillés des membres ;
- l'organisation à mettre en place pour la conduite du projet ;
- le calendrier d'intervention ;
- les livrables par étapes (titre, contenu, nombre, forme) et le taux d'avancement auquel ils correspondent ;
- les budgets-temps détaillés par intervenant et par phase, prenant en compte les participants internes au projet ;
- le plan d'assurance qualité.

Offre financière

L'offre financière comportera :

- une lettre de soumission ;
- les coûts unitaires détaillés, en faisant la distinction entre les honoraires et les frais logistiques, par intervenant et par phase ;
- le coût global de la prestation.

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.

La CRRAE-UMOA se réserve le droit de vérifier toutes les informations et d'écarter, éventuellement, tout soumissionnaire ayant fourni des informations erronées.

12. DUREE DE VALIDITE DES OFFRES

Les soumissionnaires resteront engagés par leurs offres pendant une durée de six (06) mois à compter de la date limite de dépôt des offres.

13. REGIME DE 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.

Les prestations proposées doivent prendre en compte toutes les dépenses résultant de l'exécution de la prestation, incluant tous les frais, charges, fournitures, livraisons, accessoires, démarches administratives, etc…

14. DEPOT DE DOSSIER

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 du Complexe Immobilier CRRAE-UMOA, Riviera-Bonoumin, Cocody**.

15. CONNAISSANCE DES CONDITIONS DE TRAVAIL

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.

16. CONDITIONS ET MODALITES 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 délivrée par un établissement bancaire ou une société d'assurance de premier rang. Elle serait déduite du paiement à effectuer à la livraison conforme des prestations.

Les fournisseurs préciseront les délais de livraison. 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.

17. COMPLEMENTS D'INFORMATION

Pour obtenir des renseignements destinés à une meilleure appréciation du dossier d'appel d'offres, les soumissionnaires peuvent adresser leur requête :

- **soit par télécopie au numéro 00 225 25 22 01 83 83 ;**
- **soit par messagerie électronique à l'adresse «darh@crrae.org».**

Les demandes de compléments d'informations devront être formulées par écrit, cinq (05) jours calendaires au plus tard, après la date de lancement de l'appel d'offres.

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.

ANNEXE - LISTE DES POLITIQUES ET PROCEDURES DE SECURITE DE L'INFORMATION

L'élaboration de la liste des documents de la politique générale de sécurité de l'information devra inclure au minimum les éléments suivants :

- Politique de contrôle d'accès
- Politique et procédure de gestion des actifs
- Politique et procédure de conservation des données
- Politique de conformité et protection des données
- Politique de gestion des risques liés au système d'information
- Politique de classification et de traitement des informations
- Politique de sensibilisation et de formation à la sécurité Informatique
- Politique d'utilisation acceptable des actifs
- Politique relative au travail mobile et au télétravail
- Politique de continuité des activités
- Politique et procédure de sauvegarde et de restauration
- Politique relative aux logiciels malveillants et aux antivirus
- Politique et procédure de gestion des changements
- Politique de sécurité des fournisseurs tiers
- Politique d'amélioration continue
- Politique de journalisation et de surveillance
- Politique de gestion de la sécurité du réseau
- Politique de transfert d'informations
- Politique de sécurité physique et environnementale
- Politique de gestion des clés cryptographiques
- Politique en matière de documents et d'enregistrements
- Procédure de gestion des incidents de sécurité
- Procédure de gestion des accès et habilitations
- Procédure de gestion des vulnérabilités