CAISSE RÉGIONALE DE REFINANCEMENT HYPOTHÉCAIRE

TERMES DE REFERENCE POUR LA SELECTION D'UNE FIRME POUR LA REALISATION D'EVALUATION DE SECURITE DU SYSTEME D'INFORMATION DE LA CRRH-UEMOA

Janvier 2025

I. Présentation de la CRRH-UEMOA

La Caisse Régionale de Refinancement Hypothécaire de l'Union Economique et Monétaire Ouest-Africaine (CRRH-UEMOA) est un établissement financier de crédit créé le 16 juillet 2010, et ayant pour objet social de :

- Refinancer les prêts au logement consentis par les banques ainsi que les institutions de microfinance à leurs clientèles de particuliers basés dans les huit pays de l'Union Economique et Monétaire Ouest Africaine (Côte d'Ivoire, Sénégal, Mali, Burkina Faso, Niger, Bénin, Togo, Guinée Bissau) ;
- D'émettre des obligations sur les marchés financiers et de mobiliser des ressources auprès des partenaires au développement afin de refinancer les banques ;
- Et généralement, en partenariat avec d'autres institutions, de proposer des financements alternatifs, tels que des titrisations, et des solutions de garanties.

Le capital de la CRRH-UEMOA au 30 juin 2024 est de 12 089 M FCFA. Son actionnariat compte cinquante-huit banques commerciales réparties dans les huit pays de l'UEMOA, trois institutions régionales de financement du développement (la Banque Ouest Africaine de Développement -BOAD, la Banque d'Investissement et de Développement de la CEDEAO -BIDC, et la Banque de Développement Shelter Afrique). La Société Financière Internationale (SFI ou IFC), filiale de la Banque Mondiale en charge du financement du secteur privé, est également actionnaire de la CRRH-UEMOA.

La CRRH-UEMOA a démarré ses activités opérationnelles le 16 juillet 2012. Au 31 décembre 2023, la CRRH-UEMOA a mobilisé un total de 415 milliards de FCFA pour le refinancement des portefeuilles de prêts à l'habitat des banques et institutions de microfinance dans les huit pays de l'UEMOA.

En 2017, la CRRH-UEMOA a démarré le refinancement de prêts aux logements sociaux sur ressources concessionnelles mobilisées auprès de partenaires au développement. Le montant de ses interventions dans ce cadre s'élève, à date, à 85 Mds FCFA.

Le total bilan de la CRRH-UEMOA au 30 juin 2024 est de 300 milliards de FCFA.

Basée à Lomé (Togo), la CRRH-UEMOA jouit d'un Accord de siège avec la République Togolaise qui lui accorde les privilèges et immunités reconnus aux organisations diplomatiques établies au Togo. Dans ce cadre, elle est exemptée d'impôts et taxes sur toutes les prestations et acquisitions de biens et services.

De plus amples informations sont disponibles sur le site internet de la CRRH-UEMOA, www.crrhuemoa.org.

II. Contexte et objectifs de la mission

La Caisse Régionale de Refinancement Hypothécaire de l'UEMOA (CRRH-UEMOA) s'appuie sur une infrastructure IT stratégique pour assurer la continuité et l'efficacité de ses opérations. Avec une expansion de ses activités et une dépendance accrue aux systèmes numériques, la sécurité, la performance et la résilience de notre environnement IT sont devenues des priorités essentielles.

Face à l'évolution rapide des cybermenaces et des exigences réglementaires, ainsi qu'à la nécessité de garantir une infrastructure robuste et efficace, nous avons identifié plusieurs enjeux critiques :

- **Sécurité :** Évaluer les vulnérabilités potentielles et les risques liés à nos infrastructures et applications.
- **Conformité :** Vérifier l'alignement de nos pratiques IT avec les normes internationales
- **Performance :** Identifier les éventuels goulets d'étranglement affectant nos opérations IT et proposer des optimisations
- **Evolution technologique :** Utilisation de l'IA

III. Missions

Il est attendu du prestataire, la réalisation d'une évaluation de sécurité sur l'ensemble du système d'information de la CRRH UEMOA suivant les règles de l'art. Cette évaluation couvrira trois aspects :

- Evaluation Organisationnel : il s'agira pour le cabinet d'évaluer le niveau de maturité du dispositif (ou stratégie) de sécurité de la CRRH-UEMOA pour assurer la disponibilité, la confidentialité, l'intégrité et la non-répudiation des informations.
- Evaluation technique : il s'agira de réaliser des tests d'intrusion et d'audit de configuration l'infrastructure informatique de la CRRHUEMOA afin d'identifier les vulnérabilités existantes et les risques encourue.

Le prestataire devra se baser sur les normes ISO 27001, ITIL v4 et ou COBiT comme référence de bonne pratique ou tout autre standard cohérent avec le contexte de la CRRH-UEMOA.

A l'issue des évaluations, le prestataire devra proposer à la CRRH-UEMOA un plan d'action correctives pour la mise en œuvre de toutes les recommandations formulées au cours des évaluations techniques et organisationnelle. Ce plan d'action devra :

- Identifier les actions concrètes à entreprendre et des solutions à mettre en place (humaine, organisationnelle et technique …) ;
- Indiquer les ressources (financière et humaines) nécessaires à la mise en œuvre des solutions préconisées ;
- Déterminer les priorités et l'urgence des solutions à mettre en place et définir un chronogramme de réalisation.

Le prestataire devra également faire des propositions sur l'utilisation de l'intelligence artificielle adaptés à l'activité de la CRRH-UEMOA.

IV. Portée de la mission

- **Infrastructure physique**
  - Matériels informatiques notamment poste de travail mobile ou fixe, imprimantes et les serveurs ;
  - Composants réseau : routeurs, firewall, commutateurs et le câblage ;
- **Infrastructure logique**
  - Configurations des postes et serveurs : Annuaire AD, DHCP, Tenant Azure, Tenant Office 365, PostgreSQL, SQL Server, etc. ;
  - Mécanismes d'authentification et d'autorisation d'accès aux différentes applications métier ;
  - Applications métiers
- **Système de sécurité**
  - Solutions de sauvegarde ;
  - Dispositifs de sécurité du matériel, des données et du réseau (la protection physique du local informatique, la protection antivirale, pare-feu, filtrage internet) ;
  - Référentiel de sécurité, la gestion des droits d'accès, la journalisation des accès, la maintenance informatique, etc.
- **Conformité et réglementation**
  - Respect de la législation (licences logicielles, supports, …) ;
  - Conformité des systèmes d'information à la norme ISO 27001 ;
  - Contrats de garantie et de services sur les différents composants mis en œuvre (Contrats d'assistance, contrats de maintenance des matériels, des logiciels, l'organisation de leur suivi, leur date d'expiration ou de renouvellement) et réaliser leurs évaluations coûts-bénéfices ; le cas échéant, proposer des approches contractuelles alternatives.

V. Livrables

- **Rapports d'évaluation**

Le rapport d'évaluation contiendra les recommandations et les projets susceptibles d'améliorer l'infrastructure informatique tant sur les aspects techniques qu'organisationnels, notamment :

a. Les points forts et faiblesses relevés ;
b. Le niveau de risque ;

c. Les mesures correctives ;

d. Les recommandations.

- **Feuille de route / plan d'action correctif**

L'ensemble des recommandations formulées à l'issues des évaluations devraient être proposées sous forme de plan d'action.

a. Les actions détaillées (organisationnelles et techniques) urgentes à mettre en œuvre dans l'immédiat, pour parer aux défaillances les plus graves,

b. Les actions organisationnelles, physiques et techniques à mettre en œuvre sur le court terme englobant entre autres :

- Les premières actions et mesures à entreprendre en vue d'assurer la sécurisation de l'ensemble de l'infrastructure évaluée, aussi bien sur le plan physique que sur le plan organisationnel (structures et postes à créer, opérations de sensibilisation et de formation à initier, procédures d'exploitation sécurisées à élaborer, etc.) et technique (outils et mécanismes de sécurité à mettre en œuvre), ainsi qu'éventuellement des aménagements architecturaux de la solution de sécurité existante ;
- Une estimation des formations requises et des ressources humaines, matérielles et financières nécessaires y afférentes ;

c. Un plan directeur ou une chronologie des étapes importantes à atteindre à moyen terme et les coûts associés ;

VI. Durée de la mission

- La durée de réalisation de la mission est de vingt (20) jours calendaires ; le consultant est invité à proposer un chronogramme détaillé de la réalisation de la mission.
- La mission devra démarrer cinq (05) jours ouvrables au plus tard après notification ;

VII. Profil du consultant

L'entreprise en charge du présent marché doit :

- Avoir au moins cinq (05) ans dans le domaine informatique ;
- Avoir effectué au moins deux (02) missions d'audit au cours de ces cinq dernières années
- Mettre à disposition une équipe technique qualifiée dans la réalisation de la prestation. Le personnel doit être composé à minima de :

- Un (01) chef de projet, Ingénieur en réseaux et télécommunication ou équivalent, de niveau BAC + 5 minimum, certifié PMP et d'une certification en sécurité IT, ayant au moins quatre (04) années d'expériences
- Un auditeur sécurité des systèmes d'information sénior, niveau BAC + 5 en informatique, certifié ISO 27001 LA, ITIL4, COBIT 2019, ISO 27005, EBIOS Risk Manager, WCE-P, ISO 42001 LI ; ayant au moins quinze (15) années d'expériences. Détenir les certifications ISO 31000 et ISO 27002 serait un avantage.
- Un Ingénieur pentester niveau BAC + 5, certifié CEH et SOC Analyst, ayant au moins cinq (05 années d'expériences)

Les propositions technique et financière de ce dossier d'appel d'offre devront être envoyées à l'adresse électronique suivante : consultant-it@CRRHUEMOA.ORG au plus tard le 07 février 2025 à 10H.

Les soumissionnaires enverront leurs offres protégées par mot de passe à l'adresse électronique indiquée dans le dossier. Le mot de passe sera communiqué uniquement pendant la séance d'ouverture des offres en présence des soumissionnaires.

VIII. Clause de confidentialité

Le soumissionnaire reconnaît le caractère confidentiel de toutes les informations, transmises dans le présent appel d'offres par la CRRH-UEMOA.

En conséquence, il s'engage à ne pas divulguer les informations, à ne les utiliser que dans le cadre de l'objet de l'appel d'offres, et à ne transmettre celles-ci qu'aux membres de son personnel, et/ou à ses dirigeants, administrateurs, aux membres du personnel d'une société de son groupe, à l'un quelconque de ses conseils financiers, conseils juridiques, auditeurs, ou tout autre mandataire, agent ou représentant à la condition expresse qu'il ait besoin de les connaître. Dans un tel cas, la Partie qui communique l'information à un éventuel tiers autorisé tel que mentionné ci-dessus se porte garant du respect de la confidentialité par ledit tiers.

Sous peine d'engager sa responsabilité, le Soumissionnaire s'interdit de communiquer, directement ou indirectement ou de permettre à l'un quelconque de ses employés, sous-traitants dûment autorisés de communiquer, de telles informations à un tiers sans l'accord préalable écrit de la CRRH-UEMOA.

La présente obligation de confidentialité ne s'appliquera pas à la Partie des informations : (i) accessible au public à la date de sa communication par une Partie à l'autre, ou qui viendrait à l'être postérieurement à cette date et sans faute de la Partie réceptrice; ou (ii) déjà connue de la Partie réceptrice au moment de sa communication par l'autre Partie, ou (iii) transmise à la Partie réceptrice avec dispense expresse d'obligation de confidentialité; ou (iv) fournie à la Partie réceptrice sans

obligation de confidentialité par un tiers la détenant légitimement; ou (v) obtenue par la Partie réceptrice par des développements internes indépendants entrepris de bonne foi par des membres de son personnel n'ayant pas eu accès aux informations ; (vi) aux informations nécessaires aux transferts de compétence.

La présente obligation de confidentialité restera en vigueur durant la présente consultation et pendant deux (02) années après la clôture de la présente consultation.

IX. AVERTISSEMENTS

Les soumissionnaires dont les offres n'auraient pas été retenues, seront avisés en temps opportun sans aucune obligation de justification de la part de la CRRH-UEMOA, quant au soumissionnaire retenu ni aux critères de décision.

La CRRH-UEMOA se réserve le droit de sursoir à la consultation à tout moment s'en avoir à le justifier aux prestataires.