ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

DEMANDE DE MANIFESTATIONS D'INTÉRÊT
(SERVICES DE CONSEIL - CONSULTANTS INDIVIDUELS)

PAYS : NIGERIA
NOM DU PROJET : PROGRAMME RÉGIONAL D'INTÉGRATION NUMÉRIQUE EN AFRIQUE DE L'OUEST (WARDIP)
Numéro de subvention : E264-3W

Titre de la mission : Révision de la Directive C/DIR 1/08/11 relative à la lutte contre la cybercriminalité au sein de la CEDEAO.

Numéro de référence : NG-WARDIP-ECOWAS-471324-CS-INDV

La Commission de la Communauté économique des États de l'Afrique de l'Ouest (Commission de la CEDEAO) a reçu un financement de la Banque mondiale pour la mise en œuvre du **Programme régional d'intégration numérique en Afrique de l'Ouest (WARDIP)** et a l'intention d'utiliser une partie des fonds pour des services de conseil.

Les services de conseil ("les services") comprennent la révision et la mise à jour de la Directive C/DIR 1/08/11 relative à la lutte contre la cybercriminalité, afin d'en améliorer la pertinence et l'efficacité dans la lutte contre les cybercrimes émergents. Cette révision vise à aligner la Directive sur les normes et standards internationaux récents. La mission devrait être achevée dans un délai de vingt (20) semaines.

Les termes de référence (TOR) détaillés pour la mission sont disponibles sur le *site web* suivant : https://www.ecowas.int/procurement/procurement_m/intellectual-services/

La Commission de la CEDEAO invite les Consultants individuels éligibles ("Consultants") à manifester leur intérêt à fournir les Services. Les Consultants intéressés doivent fournir des informations démontrant qu'ils ont les qualifications requises et l'expérience pertinente pour exécuter les Services. **Les qualifications et l'expérience pertinente des consultants doivent être justifiées par des documents tels que des curricula vitae signés (avec références), des diplômes, des certificats de formation, des contrats, des certificats de bonne fin d'exécution, etc. La Commission de la CEDEAO se réserve le droit de rejeter toute candidature qui ne serait pas accompagnée des pièces justificatives requises.**

Les critères d'évaluation sont les suivants :

Qualifications et compétences (preuves à l'appui) :

- Posséder au moins une Licence ou un master en droit, en droit des TIC, en droit international ou dans un domaine juridique connexe pertinent à la mission ;
- Des qualifications ou formations complémentaires pertinentes à la mission seront très appréciées ;
- Faire preuve d'excellentes compétences en communication orale, en rédaction de rapports, en présentations et en animation d'ateliers.

Expérience professionnelle (preuves à l'appui) :

- Posséder au moins sept (7) années d'expérience professionnelle ou une expertise démontrable équivalente dans le domaine de la cybercriminalité en rapport avec cette mission.

- Justifier d'une expérience avérée dans l'élaboration et la révision de cadres juridiques et réglementaires pour des organisations internationales ou régionales. Ces éléments doivent inclure des exemples de projets réussis, de publications ou de contributions à des réformes juridiques importantes.
- Démontrer une connaissance des instruments juridiques des organisations sous-régionales, continentales et internationales auxquelles les États membres de la CEDEAO sont parties, dans le domaine de la cybersécurité, de la cybercriminalité, de la protection des données personnelles, des lois sur la confidentialité et des cadres de partage de données transfrontaliers.
- Toute expérience doit être justifiée par des certificats de bonne exécution, des contrats ou des documents équivalents.

Langues :

- Le consultant doit démontrer sa maîtrise d'au moins plus d'une des langues officielles de la CEDEAO (anglais, français et portugais). La maîtrise d'une troisième langue constitue un atout supplémentaire.

L'attention des Consultants intéressés est attirée sur la Section III, paragraphes 3.14, 3.16, et 3.17 du "Règlement de passation des marchés pour les emprunteurs du FPI" de septembre 2023 de la Banque mondiale ("Règlement de passation des marchés"), qui énonce la politique de la Banque mondiale en matière de conflits d'intérêts.

Un consultant sera sélectionné conformément à la **méthode de sélection des consultants individuels** définie dans les règles de passation des marchés de la Banque mondiale.

De plus amples informations peuvent être obtenues aux adresses électroniques ci-dessous pendant les heures de services, ***de 0900 à 1700 heures, heure du Nigéria (GMT + 1).***

Les manifestations d'intérêt doivent être envoyées par écrit aux adresses ci-dessous par courrier électronique avant le **17 février 2025, à 17 h 00 GMT +1, heure du Nigeria.**

Commission de la CEDEAO
A l'attention du Commissaire Infrastructure, Energie et Digitalisation
Abuja, Nigeria
Courriel : wardiprecruitment@ecowas.int et copie pbessi@ecowas.int ; abah@ecowas.int ; mamoa@ecowas.int ; folagunju@ecowas.int ; msene@ecowas.int ; ikkamara@ecowas.int ; sbangoura@ecowas.int.

Abuja, le 30 janvier 2025

M. Sédiko DOUKA
Commissaire Infrastructure, Energie et Digitalisation

Pièce jointe : TdRs de la mission

ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Termes de référence : Révision de la Directive C/DIR 1/08/11 relative à la lutte contre la cybercriminalité au sein de la CEDEAO

1. Contexte

Les technologies numériques transforment la vie des habitants de la région, accroissent la connectivité et les opportunités, mais posent également des problèmes de sécurité. Les incidents de cybercriminalité ont augmenté, l'Afrique ayant connu la moyenne hebdomadaire la plus élevée de cyberattaques par organisation au deuxième trimestre 2023, soit une augmentation de 23 % par rapport à 2022 [1].

Interpol a identifié les principales cybermenaces en Afrique comme étant les escroqueries en ligne, l'extorsion numérique, la compromission des e-mails professionnels, les « ransomwares » et le « phishing » [2]. L'Afrique abrite 60 % des auteurs de compromission des e-mails professionnels dans le monde, six des pays les plus touchés étant situés en Afrique de l'Ouest [3]. Le rapport d'évaluation des cybermenaces africaines 2024 d'Interpol confirme que ces menaces restent répandues [4].

Les pays ont adopté des lois sur la cybercriminalité, mais la nature évolutive des cybermenaces nécessite des mises à jour continues. La directive de la CEDEAO de 2011 sur la lutte contre la cybercriminalité visait à harmoniser les lois dans toute l'Afrique de l'Ouest, mais elle doit être révisée pour répondre aux nouveaux défis et aux préoccupations en matière de droits de l'homme.

La directive initiale ne prévoyait pas de garanties pour les pratiques d'application de la loi et la coopération internationale, ce qui soulevait des problèmes de droits de l'homme. Il est essentiel de trouver un équilibre entre les mesures de sécurité et les droits individuels, ce qui nécessite de mettre à jour les pouvoirs des forces de l'ordre aux niveaux national et régional.

La CEDEAO met l'accent sur l'intégration régionale et la coopération entre les États membres. Des cadres juridiques harmonisés sont essentiels pour lutter contre la cybercriminalité et les délits numériques, tels que les crimes liés aux « ransomwares » ou aux cryptomonnaies ,

[1] https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year- selon-check-point-research/
[2] https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa
[3] Agari , La géographie du BEC. La portée mondiale de la principale cybermenace mondiale, 2020. Disponible à l'adresse : [https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec [.pdf]
[4] https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

facilitant la collaboration dans l'application de la loi, le partage de renseignements et les processus judiciaires.

Plusieurs États membres de la CEDEAO ont signé des traités internationaux sur la cybercriminalité. Il est nécessaire d'analyser ces instruments et d'y intégrer les meilleures pratiques.
La révision de la Directive garantit sa pertinence et son efficacité dans la lutte contre les cybercrimes émergents. La Commission de la CEDEAO recherche un consultant individuel pour réviser et mettre à jour la Directive C/DIR 1/08/11 relative à la lutte contre la cybercriminalité.

2. Objectifs et étendue de la mission

2.1. Objectif général

L'objectif est de réviser et de modifier la Directive C/DIR 1/08/11 relative à la lutte contre la cybercriminalité afin d'en améliorer la pertinence et l'efficacité dans la lutte contre les cybercrimes émergents. Cette révision vise à aligner la Directive sur les normes et standards internationaux récents.

2.2. Etendue de la mission

Le processus de révision impliquera :

a. Procéder à une évaluation approfondie de la directive existante de 2011 afin d'identifier les lacunes, les incohérences et les domaines à améliorer.
b. Évaluer l'efficacité et l'adéquation des dispositions actuelles de la directive C/DIR 1/08/11.
c. Aligner la Directive sur les cadres, normes et pratiques internationaux et régionaux tels que la Convention des Nations Unies contre la cybercriminalité, la Convention de l'Union africaine sur la cybersécurité et la protection des données (Convention de Malabo), la Convention de Budapest sur la cybercriminalité et ses premier et deuxième protocoles additionnels.
d. Étudier les cadres de cybercriminalité en Afrique et dans le monde pour capturer les meilleures pratiques, principes et concepts pour réviser et moderniser la directive.
e. Veiller à ce que la directive tienne compte des avancées technologiques et permette une utilisation accrue de la technologie dans la lutte contre la cybercriminalité.
f. Rédiger les dispositions mises à jour pour combler les lacunes identifiées et les menaces émergentes.
g. Animer des consultations et des ateliers pour recueillir des contributions et des commentaires.
h. Finaliser la directive révisée pour adoption par les États membres de la CEDEAO.

Le consultant est tenu de consulter toutes les parties prenantes nationales et régionales concernées.

3. Livrables et calendrier

3.1. Livrables et calendrier de mise en œuvre des services

La mission devrait être achevée dans un délai de **vingt (20) semaines** , selon le calendrier indicatif ci-dessous :

#	Livrables	Chronologie
1	Soumission du rapport initial	Signature du contrat + 2 semaines
2	Validation du rapport initial par la Commission de la CEDEAO	Signature du contrat + 4 semaines
3	Présentation des résultats de l'analyse de la directive existante, du rapport d'analyse comparative et du projet initial de la directive révisée	Signature du contrat + 8 semaines
4	Validation du projet initial de directive révisée (atelier et rapport)	Signature du contrat + 11 semaines
5	Soumission de la directive finale	Signature du contrat + 15 semaines
6	Validation du projet finalisé de directive révisée (atelier et rapport)	Signature du contrat + 18 semaines
7	Soumission de la directive finale (incorporer les commentaires)	Semaine 20

3.2. Format des rapports

1. Le consultant préparera les documents au format électronique (WORD et PDF) dans les langues précisées comme suit :
   a. Rapport initial - Anglais et Français
   b. Projet de directive révisée – anglais, français et portugais.
   c. Directive finale révisée – anglais, français et portugais.
2. Les rapports initiaux et finaux seront présentés aux experts des États membres de la CEDEAO pour validation et devront inclure les observations formulées jusqu'à ce qu'elles soient jugées satisfaisantes. Le rapport initial sera validé par la Commission de la CEDEAO.
3. Afin de faciliter la séance de validation, le consultant préparera des diapositives d'atelier résumant le contenu des rapports en anglais, en français et en portugais.

4. Consultant et obligations de la CEDEAO

4.1. Obligations du consultant

a. Toutes les ressources nécessaires à la réalisation de l'étude sont à la charge du consultant. Il convient donc d'en tenir compte lors de la préparation de la proposition.

b. Le consultant assumera l'entière responsabilité de la collecte des données auprès des États membres de la CEDEAO, des institutions de la CEDEAO et des autres parties prenantes, ainsi que de toutes les responsabilités qui pourraient être impliquées.
c. Le Consultant s'engage à vérifier la cohérence des données et informations collectées dans le cadre de l'exécution du mandat.
d. Le Consultant est tenu au respect du secret professionnel pendant et après la mission et de tenir un inventaire de tous les documents produits et mis à sa disposition.
e. Dans la méthodologie d'exécution de la mission, le Consultant devra élaborer un plan de travail prenant en compte le calendrier de mise en œuvre défini à la section 3.
f. Le calendrier de mise en œuvre fourni au point 3.4 est indicatif. Il est probable que certaines activités soient réalisées simultanément. Les propositions des consultants seront donc évaluées en fonction de leurs propositions visant à optimiser la mise en œuvre.
g. Le consultant devra animer des ateliers de validation des livrables. Les ateliers se tiendront physiquement dans une ville de l'espace CEDEAO et les dépenses liées à la participation du consultant doivent être prises en compte dans la préparation de la proposition du consultant.

4.2. Obligations de la CEDEAO

a. La Commission de la CEDEAO mettra à la disposition du Consultant tous les documents et procédures utiles à sa disposition nécessaires à l'exécution de la présente mission.
b. La CEDEAO validera la méthodologie de travail et suivra la bonne exécution de la mission.
c. La CEDEAO sera également chargée d'organiser un atelier avec les experts des États membres pour valider les livrables et accepter les conclusions de la mission.

5. Qualifications et expérience du consultant

5.1. Qualifications et compétences

- Posséder au moins une Licence ou un master en droit, en droit des TIC, en droit international ou dans un domaine juridique connexe pertinent à la mission.
- Des qualifications ou formations supplémentaires pertinentes à la mission seront très appréciées.
- Faire preuve d'excellentes compétences en communication orale, en rédaction de rapports, en présentations et en animation d'ateliers.

5.2. Expérience

- Posséder au moins sept (7) années d'expérience professionnelle ou une expertise démontrable équivalente dans le domaine de la cybercriminalité en rapport avec cette mission.

- Justifier d'une expérience avérée dans l'élaboration et la révision de cadres juridiques et réglementaires pour des organisations internationales ou régionales. Ces éléments doivent inclure des exemples de projets réussis, de publications ou de contributions à des réformes juridiques importantes.
- Démontrer une connaissance des instruments juridiques des organisations sous-régionales, continentales et internationales auxquelles les États membres de la CEDEAO sont parties, dans le domaine de la cybersécurité, de la cybercriminalité, de la protection des données personnelles, des lois sur la confidentialité et des cadres de partage de données transfrontaliers.
- Toute expérience doit être justifiée par des certificats de bonne exécution, des contrats ou des documents équivalents.

5.3. Langue

- Le consultant doit démontrer sa maîtrise d'au moins plusieurs langues officielles de la CEDEAO (anglais, français et portugais). La maîtrise d'une troisième langue constitue un atout supplémentaire.
- Le consultant (individuellement ou en équipe) doit avoir la capacité de travailler et de réviser les textes juridiques pertinents dans les langues officielles de la CEDEAO (anglais, français et portugais).
- Le recours à des experts pour la traduction peut être une option.

Remarque : Les candidats doivent fournir des CV signés (avec références), des diplômes, des attestations de formation et des attestations de mission/travail, etc.