ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Termes de Référence pour l'étude de faisabilité pour la création d'un Centre Régional de Coordination de la Cybersécurité de la CEDEAO

1. Contexte et justification

La Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), créée le 28 mai 1975 aux termes du Traité de Lagos, est l'une des cinq (5) Communautés économiques régionales (CER) de l'Union africaine. Cette organisation régionale ouest africaine regroupe quinze (15) États membres (Bénin, Burkina Faso, Cabo Verde, Côte d'Ivoire, Gambie, Ghana, Guinée, Guinée Bissau, Libéria, Mali, Niger, Nigeria, Sénégal, Sierra Leone et Togo).

La CEDEAO a pour mission de promouvoir la coopération et l'intégration dans la perspective d'une union économique en Afrique de l'Ouest afin d'élever le niveau de vie des populations, d'assurer la croissance économique, de promouvoir des relations de bon voisinage entre les États membres et de contribuer au progrès et au développement du continent africain. Pour atteindre ses objectifs, la Communauté met en œuvre des programmes, des projets et des activités dans tous les domaines socio-économiques, notamment l'agriculture, l'énergie, les transports, l'économie numérique, le commerce, la paix et la sécurité, etc.

Dans le domaine du numérique, la Commission de la CEDEAO s'est engagée dans d'importantes initiatives visant à mettre les technologies de l'information et de la communication (TIC) au service du développement. En effet, les TIC font désormais partie intégrante et sont omniprésentes dans les sociétés modernes, apportant une transformation permanente dans les modes de vie. Les TIC et les services connexes offrent un certain nombre d'avantages à la société dans son ensemble, et les applications des TIC, telles que l'administration en ligne, le commerce électronique, l'éducation et la santé en ligne, sont considérées comme des catalyseurs du développement socioéconomique. En effet, en 2018, le montant enregistré au titre de la valeur économique créée en Afrique de l'Ouest par les technologies et services mobiles se chiffre à 52 milliards de dollars US, soit

8,7 % du PIB. Selon les estimations, ce montant devrait atteindre près de 70 milliards (9,5 % du PIB) en 2025.[1]

Par ailleurs, la libéralisation du secteur des télécommunications/TIC a occasionné des progrès significatifs dans le développement des infrastructures à large bande, la pierre angulaire du développement de la connectivité régionale et internationale, et donc du développement de l'Internet.

Le taux de pénétration d'Internet en Afrique de l'Ouest est en hausse, passant de 47,44 % au 31 décembre 2019 à plus de 54 % à la fin du mois de décembre 2021. Ce taux est bien supérieur à la moyenne africaine de 43,2 %, mais reste inférieur à la moyenne mondiale de 67,9 %. Cependant, ce taux de pénétration pour l'Afrique de l'Ouest devrait augmenter avec l'essor des nouvelles technologies, la poursuite du déploiement du haut débit, ainsi que la transformation numérique initiée par les États membres, permettant ainsi aux citoyens de la Communauté de bénéficier d'un accès accru à Internet à haut débit et à travers laquelle les innovations liées aux TIC peuvent être exploitées pour la croissance économique et le développement social de la région.

Cependant, cette connectivité accrue, qui transforme nos sociétés et nos économies, expose également les États membres de la CEDEAO à des cyber-risques de plus en plus complexes et sophistiqués, causant d'énormes dommages et d'importantes pertes financières. Par exemple :

- **Au Nigeria :** Les statistiques publiées par Kaspersky en 2023 sur le paysage régional des menaces en Afrique mettent en évidence l'expérience du Nigeria. Au cours du 3e trimestre 2023, le Nigeria a connu une augmentation de 12 % des détections d'attaques de phishing par rapport au 2e trimestre. En outre, 28 % des ordinateurs des systèmes de contrôle industriel (SCI) au Nigeria ont été ciblés par des attaques au cours de la même période et 6 % des appareils de l'Internet des objets (IoT) ont été confrontés à des failles de sécurité.
- **Ghana :** En 2022, à la suite d'une attaque contre la Compagnie d'électricité du Ghana (ECG), les clients du plus grand fournisseur d'électricité du pays ont subi des coupures de courant pendant plusieurs jours en raison de la perturbation de certains systèmes.
- **Burkina Faso :** La Brigade centrale de lutte contre la cybercriminalité (BCLCC) du Burkina Faso a signalé une perte financière de 1.400.000.000 francs CFA (environ 2.327.346 $ US) due à la cybercriminalité entre mai 2020 et juin 2021.

[1] Rapport 2019, GSMA Mobile Economy West Africa

- **Côte d'Ivoire :** La Plateforme de lutte contre la cybercriminalité de Côte d'Ivoire indique une perte financière de 6.172.067.179 francs CFA (environ 10.260.383 $US) en 2020.

Le niveau de maturité en matière de cybersécurité de la plupart des États membres de la CEDEAO reste faible et pourrait accroître les défis liés à la cybercriminalité. Selon le rapport 2020 de l'Union internationale des télécommunications (UIT) sur l'indice mondial de cybersécurité (GCI) mesurant l'engagement des pays en matière de cybersécurité, seuls quatre (4) États membres (Ghana, Nigeria, Bénin et Côte d'Ivoire) ont un indice supérieur à la moyenne. Cependant, le meilleur pays de la région, le Ghana, est 4e en Afrique subsaharienne et 43e au monde. Par conséquent, il conviendrait de mettre en place de solides mesures de sécurité pour protéger les gouvernements, les entreprises, les infrastructures critiques, les données sensibles et les citoyens de la région.

Pour faire face à cette problématique, le Conseil des ministres de la CEDEAO a adopté *la Directive C/DIR.1/01/2021 relative à l'adoption de la stratégie régionale de cybersécurité et de lutte contre la cybercriminalité,* afin de tirer le meilleur parti des avancées technologiques, d'améliorer le niveau des mécanismes nationaux et régionaux de cybersécurité et de cybercriminalité, et de développer la coopération et l'assistance mutuelle entre les États membres de la région. En vue de soutenir et de promouvoir cette coopération et cette assistance mutuelle entre les États membres de la Communauté, la stratégie régionale, dans son sous-objectif 5.3, instruit la Commission, d'étudier avec les États membres la possibilité de créer, à court ou moyen terme, un Centre régional de coordination de la cybersécurité de la CEDEAO (ci-après « le Centre »).
L'étude de faisabilité déterminera comment le Centre pourrait organiser, dans la mesure du possible, la mise en commun des ressources et le partage d'informations entre les pays en vue d'atténuer les effets néfastes des incidents de cybersécurité.

La création d'un Centre régional de coordination de la cybersécurité de la CEDEAO présenterait plusieurs avantages pertinents pour la sécurité du cyberespace, notamment :

- **Amélioration de la collaboration** : Un centre de coordination régional permettrait une meilleure collaboration entre les principaux acteurs de la cybersécurité, tels que l'équipe d'intervention en cas d'incident de sécurité informatique (CSIRT) et toutes les parties prenantes impliquées dans le renforcement de la cybersécurité et la lutte contre la cybercriminalité. Cela permettra de faciliter l'échange d'informations, la coordination des actions et la mise en commun des ressources pour faire face aux cybermenaces.

- **Gestion des incidents** : Un centre régional de coordination pourrait jouer un rôle clé dans la gestion des incidents de cybersécurité. Il pourrait servir de point central pour la collecte et l'analyse des données liées aux cyberattaques, permettant une réponse rapide et efficace. Une telle coordination réduirait les temps de réponse et favoriserait une meilleure protection des infrastructures critiques au niveau régional.
- **Partage d'expertise** : La réunion des experts en cybersécurité dans un pôle régional pourrait faciliter le partage des connaissances et des bonnes pratiques. Cela permettrait aux pays et aux organisations de la région de renforcer leurs compétences en matière de cybersécurité et d'améliorer leur capacité à prévenir, à détecter et à répondre aux incidents de sécurité.
- **Sensibilisation et formation :** Le centre régional pourrait également jouer un rôle important dans la sensibilisation à la cybersécurité et la formation des acteurs concernés. Il pourrait soutenir des initiatives de sensibilisation, organiser des formations et partager des ressources éducatives pour renforcer les compétences en matière de sécurité numérique dans la région.
- **Harmonisation des réglementations :** Un centre régional de coordination pourrait soutenir l'harmonisation des réglementations et des normes de cybersécurité dans l'espace CEDEAO, favoriser la coopération transfrontalière et amener les acteurs régionaux à respecter les bonnes pratiques internationales en matière de cybersécurité et de cybercriminalité.

La Semaine du CSIRT et le Symposium de la CEDEAO sur la cybersécurité tenus en 2023 ont reconnu l'importance de la création d'un Centre régional de coordination de la cybersécurité et ont recommandé qu'une étude de faisabilité détaillée soit menée pour une décision justifiée sur la création du centre par les organes appropriés de la CEDEAO (experts, ministres sectoriels, comité de l'administration et des finances, Conseil des ministres/Conférence des Chefs d'État et de Gouvernement).

Les présents Termes de référence pour l'étude de faisabilité visent à évaluer la mise en place d'un Centre régional de coordination de la cybersécurité au sein de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) en vue de renforcer la sécurité numérique et de promouvoir la coopération régionale dans un contexte de cybermenaces croissantes.

2. Objectifs de l'étude et portée de la mission

2.1. Objectif général

L'étude vise à évaluer la faisabilité technique, économique et opérationnelle de la création d'un Centre régional de coordination de la cybersécurité pour la région. Le Centre aura pour mission de coordonner les efforts dans la gestion des cyber incidents, y compris la prévention, la détection et la réponse aux cyberattaques dans l'espace CEDEAO. Il pourra également favoriser la collaboration entre les pays membres, l'échange d'informations sur les menaces et la formation des principaux acteurs.

2.2. Objectifs spécifiques

Les objectifs spécifiques sont les suivants :

a. Comparer des projets/centres similaires au niveau mondial
b. Définir avec précision le champ d'action du Centre afin de minimiser les chevauchements et de maximiser les synergies avec d'autres initiatives régionales (par exemple, ACCRC, CUA, Smart Africa, AfricaCERT, etc.), de façon à se concentrer sur une ou deux propositions de valeur spécifiques, axées sur la demande, susceptibles de garantir le meilleur retour sur investissement.
c. Évaluer la faisabilité organisationnelle, c'est-à-dire déterminer si les parties prenantes concernées, telles que les agences gouvernementales, les entreprises privées et les autres acteurs impliqués dans la cybersécurité, sont disposées à coopérer et à participer activement au fonctionnement du Centre de coordination.
d. Évaluer les infrastructures et les technologies nécessaires à la création d'un centre de coordination de la cybersécurité.
e. Analyser la faisabilité financière en évaluant les coûts associés à la création et à l'exploitation du centre, y compris les investissements initiaux, les coûts d'entretien et les ressources humaines requises.
f. Examiner les aspects juridiques, réglementaires ou politiques à prendre en compte pour la création et le fonctionnement du centre, afin de s'assurer de sa conformité aux exigences légales.
g. Évaluer les avantages attendus du Centre de coordination de la cybersécurité, notamment l'amélioration de la coordination entre les parties prenantes, la prévention et la sensibilisation aux cyberattaques, ainsi que les potentiels risques associés.
h. Proposer une stratégie de collecte de fonds pour couvrir les coûts d'investissement et de fonctionnement du centre.

i. Proposer une structure de gouvernance du Centre de cybersécurité avec des procédures et des mécanismes de prise de décision.
j. Mettre en œuvre des indicateurs pour suivre et évaluer le rendement du Centre de coordination de la cybersécurité.
k. Établir un calendrier pour la mise en place du Centre de cybersécurité, y compris la répartition des tâches et des responsabilités entre les différents acteurs impliqués dans le centre.
l. Formuler des recommandations appropriées pour assurer la viabilité du Centre.

3. Résultats attendus et calendrier de mise en œuvre

3.1. Produits livrables et documents à produire.

Le cabinet conseil (ou le cabinet) doit produire les livrables suivants :

1. Rapport initial présentant dans les détails la méthodologie proposée (décrivant la démarche à suivre pour atteindre chaque objectif, y compris les méthodes de recherche, les stratégies de mobilisation des intervenants et les techniques d'analyse des données), le calendrier et les ressources pour la réalisation de l'étude de faisabilité.
2. Rapport préliminaire décrivant les initiatives régionales existantes et attendues en matière de cybersécurité et les synergies potentielles associées, l'écosystème du CSIRT dans l'espace CEDEAO ainsi que les acteurs de la cybersécurité et de lutte contre la cybercriminalité, les principaux facteurs de succès et les défis à la mise en place et au fonctionnement d'un centre régional de cybersécurité.
3. Un projet de rapport final de l'étude de faisabilité contenant les exigences techniques, les coûts, les aspects juridiques, réglementaires et politiques et les mécanismes permettant de soutenir la création et le fonctionnement du centre.
4. Un rapport final prenant en compte les observations formulées lors de l'atelier de validation du projet de rapport.

Le consultant préparera les documents en format électronique (WORD et PDF) dans les versions linguistiques spécifiées ci-dessous :

1. Rapport initial – anglais ou français
2. Rapport préliminaire – anglais, français et portugais.
3. Projet de rapport final – anglais, français et portugais.
4. Rapport final – anglais, français et portugais.

Le rapport préliminaire et le projet de rapport final seront présentés aux experts des États membres pour validation et ils devront inclure les commentaires formulés et ne seront supprimés que lorsqu'ils seront jugés satisfaisants. Le rapport initial sera validé par la Commission de la CEDEAO.

3.2. Calendrier de mise en œuvre de l'étude de faisabilité

La durée de la mission ne doit pas excéder vingt (20) semaines, et sera réalisée selon le calendrier indicatif ci-dessous :

Calendrier	Produits livrables
Signature du contrat + 2 semaines.	Rapport initial détaillant la méthodologie, le calendrier et les ressources proposés pour la réalisation de l'étude de faisabilité.
Signature du contrat + 4 semaines	Validation du rapport par la Commission de la CEDEAO
Signature du contrat + 12 semaines	Rapport préliminaire présentant l'écosystème du CSIRT dans l'espace CEDEAO ainsi que les acteurs de la cybersécurité et de lutte contre la cybercriminalité, les principaux facteurs de succès, les défis à la mise en place et au fonctionnement d'un hub régional de cybersécurité
Signature du contrat + 16 semaines	Validation (virtuelle) du rapport préliminaire par les États membres
Signature du contrat + 20 semaines	Projet de rapport final de l'étude de faisabilité contenant les exigences techniques, les coûts, les aspects juridiques, réglementaires et politiques et les mécanismes de viabilité pour la création et le fonctionnement du Centre
Signature du contrat + 22 semaines	Validation du projet de rapport final par les États membres
Signature du contrat + 24 semaines	Soumission du rapport final (dans les 3 langues officielles de la CEDEAO) en tenant compte des observations issues de l'atelier de validation du projet de rapport.

Outre la soumission des produits livrables, le consultant communiquera régulièrement avec le gestionnaire de projet de la CEDEAO.

4. OBLIGATIONS DES CONSULTANTS ET DE LA CEDEAO

4.1. Obligations du cabinet conseil

a. Toutes les ressources nécessaires à la réalisation de l'étude sont à la charge du cabinet conseil. Il convient d'en tenir compte dans la préparation de l'offre.
b. Le Cabinet assume l'entière responsabilité de la collecte des données auprès des États membres et des institutions/agences de la CEDEAO, ainsi que de toutes les responsabilités qui pourraient en découler.
c. Le Cabinet vérifie les données et informations collectées dans le cadre de l'exécution de la mission.
d. Dans la méthodologie d'exécution de la mission, le cabinet établit un plan de travail qui tient compte du calendrier de mise en œuvre fixé au paragraphe 3.2.
e. Le cabinet est tenu au secret professionnel pendant et après l'exécution de la mission et tient un inventaire de tous les documents produits et de ceux mis à sa disposition.
f. Le cabinet devra animer les ateliers de validation organisés avec les États membres.

4.2. Obligations de la CEDEAO

a. La Commission de la CEDEAO mettra à la disposition du cabinet toute la documentation et les procédures utiles dont elle dispose et qui sont nécessaires à l'exécution de la présente mission.
b. La Commission doit faciliter l'introduction du cabinet dans les États membres.
c. Elle valide la méthodologie de travail et surveille la bonne exécution de la mission.
d. Elle organisera un atelier avec les experts des États membres pour valider les produits livrables et accepter les conclusions des travaux.

5. PROFIL DU CABINET CONSEIL

5.1. Qualifications du cabinet/des consultants

Cette mission requiert des cabinets ayant une solide expérience dans le secteur du numérique et une bonne compréhension des enjeux et des opportunités inhérents au domaine de la cybersécurité, ainsi que des connaissances et une expérience avérées dans les domaines de la gouvernance, de la législation, de la gestion des risques, de la protection des infrastructures critiques de l'information, de la réponse aux incidents et du développement des compétences en cybersécurité.

La réalisation de projets de politique de cybersécurité, l'élaboration de documents d'architecture de cybersécurité, seront des critères importants dans le choix du cabinet. À ce titre, les cabinets concernés devront justifier d'au moins cinq (5) années d'expérience dans le domaine du conseil. Ils devront également avoir travaillé sur au moins un (1) projet de cybersécurité au cours des cinq (05) dernières années.

5.2. Qualification de l'équipe

Le cabinet proposera une équipe de base composé comme suit :

- Un (1) chef d'équipe/gestionnaire de projet ;
- Un spécialiste de l'analyse des cybermenaces et de la gestion des incidents ;
- Un spécialiste de la politique et de la gouvernance en matière de cybersécurité ;
- Un juriste spécialisé dans la cybersécurité (expert en réglementation).

L'équipe de consultants devrait avoir la capacité d'analyser les besoins spécifiques de la CEDEAO et de formuler des recommandations appropriées pour la création d'un centre efficace.

Gestionnaire de projet

Un (1) gestionnaire de projet expérimenté dans la gestion de projets de cybersécurité et possédant une bonne connaissance des bonnes pratiques mondiales en matière d'élaboration de politiques de cybersécurité. Il sera responsable de la supervision de l'ensemble de l'étude de faisabilité. Il devra coordonner avec tous les experts, gérer les délais, allouer les ressources et veiller à la bonne exécution du projet. Il/elle sera chargé(e) d'analyser la viabilité de la mise en place du Centre et doit avoir préalablement travaillé avec des institutions gouvernementales, notamment dans l'espace CEDEAO. Il doit être titulaire d'au moins un master et justifier de dix (10) années d'expérience dans le secteur de l'économie numérique. De plus, il doit justifier d'au moins cinq (5) années d'expérience professionnelle pertinente dans le domaine de la cybersécurité.

Juriste spécialisé dans la cybersécurité

Il doit avoir des connaissances et justifier d'une expérience avérées dans l'analyse des cadres juridiques et réglementaires dans les pays en développement. La connaissance des exigences légales et réglementaires pertinentes, telles que les réglementations en matière de protection des données et du système juridique ouest-africain est hautement souhaitée.

Il/elle devra avoir une bonne compréhension des exigences et une connaissance des implications juridiques des politiques et mesures de cybersécurité, y compris les stratégies de cybersécurité et la mise en place de CSIRT. Le juriste sera chargé de déterminer les considérations juridiques, réglementaires ou politiques qui doivent être prises en compte lors de la création et du fonctionnement du Centre. Il doit être titulaire d'au moins un master en droit et justifier de huit (8) années d'expérience dans le secteur de l'économie numérique, dont cinq (5) années dans les domaines de la cybersécurité et de la cybercriminalité.

Spécialiste de la politique et de la gouvernance en matière de cybersécurité

Le candidat idéal pour ce poste doit avoir une connaissance approfondie des bonnes pratiques en matière de sécurité informatique, des cybermenaces actuelles et des stratégies de prévention des cyberattaques. Il doit avoir une maîtrise des politiques et des normes de cybersécurité aux niveaux national, régional et international, et la capacité de mener des analyses approfondies des risques de cybersécurité et d'identifier les potentielles vulnérabilités. La possession d'une expérience en matière de réponse aux incidents de cybersécurité serait souhaitable, en particulier en ce qui concerne la mise en place et la gestion des CSIRT. De plus, il doit être titulaire d'au moins une maîtrise en informatique, en génie logiciel, en cybersécurité/sécurité de l'information ou dans tous autres domaines pertinents et justifier d'au moins cinq (5) années d'expérience dans le domaine de la politique et de la gouvernance de la cybersécurité. Des certifications ou des formations sur des sujets de cybersécurité seraient un avantage supplémentaire.

Spécialiste de l'analyse des cybermenaces et de la gestion des incidents

Le candidat idéal pour ce poste doit avoir une connaissance approfondie des cybermenaces et des techniques d'attaque, posséder des compétences en analyse des risques pour identifier les actifs critiques, les vulnérabilités et déterminer les impacts potentiels d'une attaque, et une connaissance approfondie des principes fondamentaux de la sécurité informatique, des protocoles réseau, des systèmes d'exploitation et de la sécurité des applications. Il doit être titulaire d'au moins un master (ou de tout autre diplôme équivalent) en sécurité informatique, en génie logiciel ou dans toute discipline similaire d'une université reconnue et justifier d'au moins cinq (5) années d'expérience professionnelle dans le domaine de la cybersécurité, avec une spécialisation en gestion du CSIRT. La possession de certifications ou des formations dans des sujets de cybersécurité serait un avantage supplémentaire.

Chaque membre de l'équipe doit avoir une bonne maîtrise d'au moins l’une des langues officielles de la CEDEAO (anglais, français et portugais). La connaissance pratique de l'une des deux autres langues officielles serait un avantage.