République Islamique de Mauritanie

Honneur – Fraternité – Justice

Ministère de la Transformation Numérique, de l'Innovation et de la Modernisation de l'Administration

Projet Régional d'Intégration Numérique en Afrique de l'Ouest
WARDIP – Composante Mauritanie

Unité de Gestion du Projet WARCIP-Mauritanie

TERMES DE REFERENCE (TDR)

Sélection d'un Consultant pour la réalisation d'une étude de faisabilité pour la mise en place d'une équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et d'un centre d'opérations de cybersécurité (SOC) et élaboration des cahier des charges correspondants d'un programme de renforcement de capacités et de sensibilisation dans la cybersécurité

Septembre 2023

1. Contexte

Le Gouvernement de la République Islamique de Mauritanie, avec l'appui de la Banque Mondiale, a intégré le Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP) pour promouvoir la mise en œuvre de la stratégie de transformation numérique du Pays qui vise à développer la pénétration de l'Internet haut débit, des services financiers numériques et des services en ligne (e-Gouvernement).

Le Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP) – Composante Mauritanie, (ci-après le « **Projet** ») à travers des actions impliquant les pays de la sous-région, vise spécifiquement à :

a) créer un environnement propice au bon développement d'infrastructures numériques adéquates grâce à l'adaptation du cadre juridique et institutionnel du secteur du numérique et son harmonisation en particulier pour la connectivité et les données,

(b) développer les réseaux à large bande et les services d'internet et de transit à travers le déploiement de réseaux backbones en fibre optique interconnectés au niveau régional,

(c) simplifier l'accès aux services ligne tel que le e-commerce ainsi que les services publics par le développement d'un environnement favorable et la mise en place de plateformes e-Gouvernement dans une approche de mutualisation et de coordination régionale,

d) développer les compétences dans le domaine du numérique.

La composante Mauritanienne du Programme Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP – Mauritanie) vise à élargir l'accès aux services haut débit et numériques grâce au développement et à l'intégration des marchés numériques du pays avec ceux de la région de l'Afrique de l'Ouest. Le projet est axé sur 3 éléments essentiels à l'intégration des technologies numériques au niveau régional : le marché de la connectivité, le marché des données et le marché en ligne. Il s'agira ainsi de (i) poursuivre les efforts entamés dans le cadre du Projet WARCIP-Mauritanie pour étendre la connectivité, diminuer le coût et améliorer la qualité de service, (ii) permettre l'échange, le stockage et le traitement sécurisés des données au-delà des frontières, et soutenir le déploiement régional et l'accès aux services et à l'innovation basés sur les données ; et (iii) développer l'accès et la fourniture des services en ligne publics et privés, et établir un commerce électronique transparent et sécurisé au niveau régional.

Pour atteindre ces objectifs, le Projet est structuré autour des composantes et sous-composantes suivantes :

- **Composante-1 « Développement et intégration du marché de la connectivité »** qui soutiendra les réformes visant à réduire les obstacles à la fourniture de services de télécommunications transfrontaliers par le biais de marchés ouverts ainsi que le déploiement de l'infrastructure de connectivité à large bande dans le cadre d'une approche MFD (Maximisation des Financements pour l'Investissement). Les infrastructures à large bande, telles que les réseaux à fibre optique et mobiles, ainsi que les services à large bande, gagneront grandement d'une approche prônant la mutualisation d'investissements à de plus grandes échelles avec un partage d'infrastructure dans un environnement garantissant l'accès ouvert. Les économies d'échelle d'un marché régionalement intégré pourraient également attirer davantage d'investissements privés. Une concurrence accrue permettrait une baisse des prix des services de connectivité de gros, puis de détail, dans la région. Des prix plus abordables

contribueraient à leur tour à élargir l'accès et à stimuler la demande de services connexes, générant une augmentation du trafic de données et de l'activité en ligne essentielles à la rentabilisation de nouveaux investissements dans le réseau et l'expansion de la couverture vers de nouvelles régions. Cela peut aider à combler les déficits des pays enclavés ou proches de la fracture urbaine-rurale, qui est un levier clé pour la création d'emplois et la promotion d'une croissance économique inclusive. Une connectivité à moindre coût et plus accessible ouvrirait également la voie à des services plus innovants et à des entreprises numériques qui s'appuient sur une capacité de bande passante plus élevée, renforçant encore ce cercle vertueux. Conformément aux objectifs régionaux, cette composante pourrait éventuellement inclure un soutien aux objectifs nationaux qui seraient essentiels pour tracer la voie de l'intégration.

- ✓ **La sous-composante 1.1 : Renforcement de l'environnement propice au développement et à l'intégration du marché de la connectivité** à travers des assistances techniques pour le renforcement de la connectivité nationale et internationale en conformité avec les principes du partenariat publique-privée et de l'accès ouvert et non discriminatoire et conformément aux standards internationaux et régionaux. La sous-composante ciblera également à renforcer le cadre règlementaire pour assurer un accès compétitif aux Infrastructures numérique à travers des modèles de partage des infrastructures, et le développement des modèles de gros.
- ✓ **La sous-composante 1.2 : Soutien du marché de la connectivité** sera essentiellement consacrée au financement des Infrastructures étudiées dans le cadre de la sous composante 1.1, tel que les tronçons manquants prioritaires de la dorsale nationale, le raccordement au réseau régional ainsi que les possibilités d'extension du réseau fibre optique dans certaines zones urbaines en complément des investissements privés.

- **Composante 2 « Développement et intégration du marché des données »** qui vise à permettre l'échange, le stockage et le traitement sécurisés des données à travers les frontières pour soutenir le déploiement régional et l'accès aux services, à l'innovation et à l'infrastructure axés sur les données, la réduction des restrictions régionales sur la libre circulation des données et l'augmentation des investissements dans l'infrastructure de données. Il est donc essentiel d'améliorer l'environnement juridique et réglementaire de la cybersécurité, ainsi que la protection des données et de la vie privée. Un marché des données plus intégré en Afrique de l'Ouest pourrait stimuler l'innovation et améliorer l'analyse des données, ce qui se traduirait par des avantages économiques et sociaux importants et des gains d'efficacité dans pratiquement tous les secteurs. La création d'un marché des données plus vaste générerait également des réductions de coûts substantielles en créant des économies d'échelle qui rendraient les investissements dans les centres de données régionaux qui prennent en charge les services en ligne, y compris l'hébergement en nuage, plus viables financièrement. Conformément aux objectifs régionaux, cette composante pourrait éventuellement inclure un soutien aux objectifs nationaux qui seraient essentiels pour favoriser l'intégration.
  - ✓ **La sous-composante 2.1 : Création d'un environnement propice au développement et à l'intégration du marché des données** cible principalement à développer une règlementation des données et un cadre d'interopérabilité qui soient conformes aux dispositions régionales et internationales. La sous composante cible également à renforcer

les aspects de cybersécurité et la protection des données à travers des activités d'appui pour le renforcement des compétences et des structures en charge de ces aspects.

- ✓ **La sous-composante 2.2: Soutien du marché des données** sera consacrée au financement des infrastructures essentielles et des plateformes, pour le développement du marché des données (identifiées dans la sous-composante 2.1), et l'acquisition des équipements techniques.

- **Composante 3 « Développement et intégration du marché en ligne »** qui vise à soutenir le développement et l'intégration du marché en ligne, ce qui créera un environnement propice à la fourniture et à l'accès transfrontaliers de biens ou de services numériques. Cette composante aiderait les gouvernements, les entreprises et les citoyens des pays participants à accéder et à fournir des services privés et publics en ligne, ainsi qu'à effectuer des achats en ligne de manière transparente depuis n'importe où dans la région. Lorsqu'elles sont reconnues au-delà des frontières par le biais de cadres régionaux, les signatures électroniques peuvent accélérer le commerce et l'intégration en permettant des transactions transfrontalières sécurisées. Cela contribuerait également à permettre les paiements et le commerce transfrontaliers, que cette composante renforcera encore en réduisant les obstacles supplémentaires autour des transactions transfrontalières et en renforçant la coordination régionale, en particulier sur les paiements numériques et d'autres services financiers numériques. Les paiements numériques doivent être soutenus par un cadre juridique solide et proportionné pour garantir leur fonctionnement efficace. Dans ce contexte, des cadres réglementaires basés sur les bonnes pratiques et les normes internationales doivent être en place et harmonisés au niveau régional pour être applicables dans tous les pays. En outre, la composante soutiendrait également le déploiement de services numériques publics clés pour aider les citoyens et les entreprises à rationaliser l'interaction en ligne avec le gouvernement, conformément aux normes numériques élaborées au niveau régional pour faciliter les flux transfrontaliers régionaux et l'échange de données. Les compétences numériques sont essentielles pour stimuler l'adoption des technologies, l'innovation numérique et l'entrepreneuriat, qui seraient soutenus dans le cadre de cette composante en ciblant les secteurs économiques prioritaires régionaux stratégiques, tels que l'agriculture et le tourisme. En conséquence, les citoyens et les entreprises auraient un accès plus large à une gamme plus large de services numériques. Conformément aux objectifs régionaux, cette composante pourrait éventuellement inclure un soutien aux objectifs nationaux qui seraient essentiels pour favoriser l'intégration. Il convient également de noter que de nombreuses activités relevant de cette composante contribueront à la réduction des émissions des GES (Gaz à Effet de Serre) provenant des besoins de transport en raison de la disponibilité du marché en ligne permettant l'accès à distance aux biens ou services.

  - ✓ **La sous-composante 3.1 : Création d'un environnement propice au développement et à l'intégration du marché en ligne** va cibler le développement des services financiers numériques et les fintechs et du commerce électronique. La sous-composante comprendra un appui réglementaire et des programmes d'innovation et de renforcement des capacités, ainsi qu'un appui technique pour soutenir les structures clés et développer les services en ligne prioritaires.
  - ✓ **La sous-composante 3.2 : Accompagnement du marché en ligne** sera essentiellement consacrée au financement des activités de la sous-composante 3.1 dont les programmes

d'innovation et de renforcement des capacités et éléments clés pour développer les services en ligne prioritaires.

- **Composante 4 : « Gestion de projet ».** Cette composante financera diverses activités liées aux aspects environnementaux et sociaux, et fiduciaires, au renforcement des capacités et le soutien à la mise en œuvre du Projet. Elle vise à fournir une assistance technique et un renforcement des capacités pour la préparation et la mise en œuvre du programme. Elle financera les coûts de fonctionnement de l'Unité d'Exécution du Projet (UEP) pour le pays. Un soutien sera fourni pour assurer la mise en place d'une capacité adéquate de sauvegardes sociales et environnementales, ainsi que fiduciaire, technique, et de suivi et d'évaluation (S&E).
- **Composante 5 : « Composante d'intervention d'urgence contingente CERC ».** Dans le contexte de la crise du COVID-19, une composante d'intervention d'urgence contingente (CERC) est ajoutée à la structure du projet pour fournir un soutien aux pays participants pour répondre aux urgences, y compris la crise du COVID-19.Elle aura une valeur initiale nulle mais pourra être financée pendant la mise en œuvre du projet pour permettre une réponse agile aux événements émergents, avec des fonds redirigés depuis d'autres composantes. L'inclusion du CERC au stade de la préparation, bien qu'avec un financement nul, offre la flexibilité nécessaire pour répondre à une urgence imminente ou réelle (telle que la COVID-19). Les dépenses de réponse à la crise pourraient couvrir, par exemple, la facilitation des paiements d'urgence aux groupes vulnérables de la population en utilisant l'argent mobile ; assurer la continuité des activités des fonctions gouvernementales essentielles, lorsque les fonctionnaires sont tenus de continuer à travailler à domicile ; ou le soutien aux MTPE, en particulier les plus touchées, pour résoudre leurs problèmes de liquidité immédiats, réduire les licenciements et éviter les faillites. Le CERC n'est pas censé financer des travaux de génie civil pouvant induire des risques et/ou des impacts environnementaux et sociaux négatifs.

Le Projet est sous la tutelle du Ministère de la Transformation Numérique, de l'Innovation et de la Modernisation de l'Administration (MTNIMA). Il est mis en œuvre par son Unité de Gestion de Projet (UGP).

Dans le cadre de la composante 2 « Développement et intégration du marché des données », le Projet cherche à recruter un Consultant (firme) qui assistera le Gouvernement Mauritanien pour réaliser (i) une étude de faisabilité et cahier des charges pour la mise en place d'une équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et d'un centre d'opérations de cybersécurité (SOC) et (ii) un programme de renforcement de capacités et de sensibilisation en cybersécurité

En effet, devant une dépendance croissante de nos sociétés modernes aux technologies numériques et le développement des risques et des menaces liés à l'usage de ces technologies, il devient urgent de se doter des outils essentiels pour répondre à cette situation.

La Mauritanie a, dans ce cadre, élaboré en 2022, une stratégie nationale de sécurité numérique pour la période 2022-2025 dont les principaux Objectifs Stratégiques sont de :

- OS1 : Doter la Mauritanie des institutions nécessaires à sa sécurité numérique,
- OS2 : Renforcer la sécurité du cyberespace mauritanien et des infrastructures critiques,
- OS3 : Renforcer le dispositif national de lutte contre la cybercriminalité,

- 0S4 : Développer la sensibilisation et les compétences,
- OS5 : Développer la collaboration nationale,
- OS6 : Développer la coopération régionale et internationale.

La mise en place d'une équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et d'un centre d'opérations de cyber sécurité (SOC) constituent deux projets importants de cette Stratégie.

2. Objectifs de l'étude

L'objectif principal de la mission est d'élaborer un plan d'établissement du CSIRT (équipe nationale d'intervention en cas d'urgence informatique) et du SOC (centre d'opérations de cyber sécurité) pour le réseau du Gouvernement (RIAD) et l'établissement d'un programme de renforcement de capacités et de sensibilisation et cahier des charges pour la mise en place d'une équipe nationale d'intervention en cas d'urgence informatique (CSIRT) et d'un centre d'opérations de cybersécurité (SOC).

Le consultant intégrera les bonnes pratiques largement rependues pour permettre au CSIRT national établi dans le cadre du plan, de participer aux initiatives et forums de coopération internationale (par exemple, FIRST). Pour atteindre cet objectif, le Projet cherche une firme ayant une solide expérience dans la création de CSIRT et SOC, en particulier dans les pays en voie de développement.

3. Mission du Consultant

Les livrables de cette mission serviraient notamment à favoriser la mise en place d'un CSIRT et d'un SOC dans le pays. Le consultant est censé effectuer les tâches suivantes :

1. Préparer l'évaluation sur site : le consultant mènera des études et des analyses sur les capacités actuelles de réponse aux incidents du pays, ainsi que sur l'état général de la cybersécurité. Les données et documents pertinents peuvent être demandés au Projet ou consultés par le biais d'une recherche documentaire s'ils sont disponibles. Des comparaisons sont à faire avec des pays de la sous-région ou des pays analogues sur la base d'un benchmark que le Consultant doit effectuer. Cette tâche comprendra la préparation d'une liste des parties prenantes concernées à interroger lors des ateliers de consultation.
2. Organiser des ateliers de consultation et de vulgarisation du CSIRT et du SOC avec les parties prenantes nationales et régionales concernées : le consultant organisera une série d'interactions et de discussions avec les parties prenantes concernées pour évaluer le niveau de préparation à la création d'un CSIRT national. Dans cette activité, le consultant mènera des entretiens, posera des questions sur les besoins et discutera des lacunes existantes et des solutions possibles. Cette tâche informera les tâches 4 et 5.
3. Audit du réseau intranet du Gouvernement : le Consultant procédera à un audit du réseau intranet de l'Administration afin de déterminer comment un SOC sera mis en place et analysera les risques de sécurité dans l'environnement informatique de l'Administration dans le but de définir le plan d'implémentation et d'opérationnalisation du SOC grâce à une approche orientée risque.
4. Elaborer le Rapport d'évaluation du niveau de préparation : le consultant préparera un rapport basé sur les informations recueillies dans les tâches 1, 2 et 3. Le rapport fournira un aperçu des capacités de réponse aux incidents existantes dans le pays, soulignera les

exigences préliminaires (par exemple, mandat, gouvernance, feuille de route, budget) pour le plan d'établissement du CSIRT et du SOC, et fournira des informations sur le contexte plus large de la cybersécurité et définira le périmètre et les spécifications fonctionnelles du CSIRT et du SOC y compris la définition des contraintes techniques, organisationnelles, légales et réglementaires du CERT National et du SOC.

5. Proposition de l'architecture et rédaction du cahier des charges du SOC : le Consultant procédera à la proposition de plusieurs modèles d'architecture et à l'élaboration du cahier des charges du SOC et au Document d'appel d'offres correspondant. Une fonctionnalité supplémentaire que le Consultant doit décrire dans ce cadre est celle de mise en place d'un système de filtrage des contenus internet afin de pouvoir appliquer des politiques de navigation au niveau national.
6. Rédiger le plan d'établissement du CSIRT et du SOC : le consultant élaborera un plan complet qui définit les services, le public cible, les ressources nécessaires et d'autres éléments pertinents pour établir un CSIRT national dans le pays et un SOC pour le réseau administratif (Intranet). Le consultant fournira également une feuille de route étape par étape pour la mise en œuvre du plan avec un séquencement claire et un timeline d'implémentation.
7. Etablissement des besoins en ressources humaines et qualifications.
8. Etablissement des procédures de fonctionnement, de la plage d'intervention (24x7 ou pas suivant la priorité et l'urgence), des niveaux de services (Service Level Agreement ou SLA) des indicateurs et reporting attendus.
9. Elaboration du budget détaillé de mise en place et de fonctionnement.
10. Etablissement du modèle de gouvernance et de gestion du CSIRT / SOC sur la base de benchmark et détermination des fonctionnalités gérées en interne et celles externalisées et le cas échéant, comment la gestion pourrait être faite en collaboration avec les instances privées (assistance à l'exploitation, support de haut niveau pour l'équipe, fourniture de service au profit du privé, …) en tenant compte des lois et règlementations en vigueur.
11. Proposer un catalogue de services pour répondre aux besoins actuels et futurs des ministères et éventuellement des entités privées avec les différents SLA.
12. Définir un modèle économique pour assurer la commercialisation et la continuité des services.
13. Elaboration d'un programme de formation pour les équipes qui seront chargées de la gestion du SOC/CSIRT. Ce plan de formation doit être détaillé et prenant en compte les besoins de montée en compétences graduelle et la disponibilité de la documentation nécessaire pour la montée en compétence des futurs ressources.
14. Rapport au chef de projet : le consultant rendra compte régulièrement au chef de projet et fournira des rapports de mise à jour sur l'état d'avancement, des présentations et d'autres formes de communication, au besoin.
15. Autres tâches applicables : le consultant effectuera toutes les tâches supplémentaires demandées par le chef de projet dans le cadre des livrables décrits dans les présents termes de référence,

16. Elaboration d'un programme de renforcement de capacités et de sensibilisation dans le domaine de la cybersécurité. Ce la comprend :

    a. Analyse des Besoins:
        i. Évaluation des connaissances et compétences actuelles des fonctionnaires techniques (IT) des Départements ministériels en matière de cybersécurité.
        ii. Évaluation de la sensibilisation actuelle du grand public à la cybersécurité.
    b. Définition des Objectifs :
        i. Pour les fonctionnaires : le programme doit permettre l'amélioration des compétences techniques, compréhension des politiques et réglementations, l'identification de plateformes de certification et plans détaillées pour la certification, etc.
        ii. Pour le grand public : le programme doit inclure un volet de sensibilisation aux risques en ligne, adoption de bonnes pratiques, etc.
    c. Identification des Groupes Cibles :
        i. Ciblage des départements ou fonctions spécifiques parmi les fonctionnaires.
        ii. Segmentations du grand public (jeunes, seniors, parents, etc.) pour des campagnes ciblées.
    d. Élaboration du Contenu :
        i. Pour les fonctionnaires : Elaboration des programmes de formations détaillées, ateliers pratiques, études de cas, etc.
        ii. Pour le grand public : Elaboration des brochures, vidéos, webinaires, jeux éducatifs, etc.
    e. Choix des Canaux de Diffusion :
        i. Pour les fonctionnaires : Identification et élaboration du plan détaillé pour la mise en place de plateformes de e-learning, sessions de formation en présentiel, etc.
        ii. Pour le grand public : Elaboration des spécifications détaillées et des plans pour l'exploitation des médias sociaux, télévision, radio, événements communautaires, etc.

4. Conformité aux normes et bonnes pratiques internationalement reconnues

Toutes les activités et livrables mentionnés dans les présents TdR doivent être réalisés conformément aux principales normes et bonnes pratiques internationalement reconnues. L'annexe B présente une liste indicative de ressources.

5. LIVRABLES

Le consultant doit produire les livrables suivants :

- Livrable 1 : Liste des parties prenantes nationales et régionales à inviter aux ateliers de consultation et de présentation du CSIRT et SOC. La liste sera convenue avec l'Unité de Gestion du Projet WARDIP (UGP ou UGP WARDIP). L'annexe A fourni une liste des parties prenantes possibles qui devraient être prises en compte

- Livrable 2 : Atelier de concertation avec les acteurs nationaux et régionaux et de vulgarisation de ce que c'est que les CSIRT et les SOC ainsi que les rôles et responsabilités des acteurs (jusqu'à 3 jours). L'UGP soutiendra l'organisation des ateliers.
- Livrable 3 : Rapport d'évaluation de l'état de préparation / étude de faisabilité. Ce rapport comprendra les éléments suivants :
  - Résultats du benchmark effectué par le Consultant,
  - Bref examen des capacités existantes de réponse aux incidents,
  - Mandat préliminaire,
  - Structure de gouvernance,
  - Exigence pour l'organisation et l'hébergement du CSIRT et du SOC,
  - Feuille de route et budget de haut niveau,
  - Exigences de haut niveau pour la phase de conception
  - Faisabilité.
- Livrable 4 : Rapport d'audit de l'Intranet. Ce rapport traitera de l'analyse de l'architecture réseau, des serveurs d'Administration et des systèmes de gestion de l'Intranet.
- Livrable 5 : Cahier des charges pour la mise en place du CSIRT et du SOC et des interfaces et du Document d'appel d'offres. Ce cahier des charges doit établir la liste et les spécifications détaillées des fournitures et services à acquérir pour l'établissement du CSIRT et du SOC et les exigences en termes de passation des marchés. Une fonctionnalité supplémentaire que le Consultant doit décrire dans ce cadre est celle de mise en place d'un système de filtrage des contenus internet afin de pouvoir appliquer des politiques de navigation au niveau national.
- Livrable 6 : Plan d'implémentation du CSIRT et du SOC. Le plan comprendra les éléments suivants :
  - Mandat détaillé,
  - Plan de services CSIRT et du SOC,
  - Plan des processus et flux de travail CSIRT et du SOC,
  - Schéma d'organisation, de compétences et de formation du CSIRT et du SOC,
  - Plan des installations du CSIRT et du SOC,
  - Plan d'automatisation des technologies et des processus du CSIRT et du SOC,
  - Plan de coopération du CSIRT et du SOC,
  - Plan de gestion de la sécurité informatique et de l'information du CSIRT et du SOC,
  - Spécification des sites d'implémentation du CSIRT et du SOC ;
  - Feuille de route détaillée et exigences pour la phase de mise en œuvre du CSIRT et du SOC.

- Livrable 7 : Plan d'affaires et catalogue de services. Le plan comprendra les éléments suivants :
    - Le modèle technico-commercial et financier
    - Le modèle technico-commercial et financier au format Excel:
    - La restitution du modèle avec les hypothèses, paramètres, résultats…. ;
    - Les services avec les tarifs associés.

Ce plan d'affaires, sur une durée d'au moins 5 ans (idéalement 10 ans), seront réalisés au format Excel et prendront en compte/identifieront :

- Livrable 8 : Assistance à l'évaluation et suivi de la mise en œuvre : le Consultant assistera l'UGP pour l'évaluation des dossiers de sélection de l'entité qui sera chargée de mettre en place le SOC et le CSIRT et dans la phase de suivi de la mise en œuvre.
- Livrable 9 : Plan de formation, rapport final et atelier de restitution du rapport final (atelier d'un jour),
- Livrable 10 : Programme de renforcement de capacités et de sensibilisation :
    - L'élaboration d'un programme de renforcement des capacités des équipes du Ministère, des unités opérationnelles et de l'Agence en charge de la cybersécurité ;
    - L'élaboration d'un programme de sensibilisation pour le public dans les domaines de la cybersécurité et de la cybercriminalité ;
    - L'identification des plateformes et contenus de ces plateformes pour offrir un programme d'autoformation permettant de réaliser certaines certifications que le Consultant doit soumettre à la validation du Client.

Le Consultant après la validation du périmètre exact de la mission avec le maître d'ouvrage avant le démarrage, est responsable de :

- l'élaboration des documents de travail ;
- l'identification des interlocuteurs à rencontrer ;
- l'identification et la collecte des informations inhérentes à l'exécution de la mission ;
- la gestion des entretiens avec les parties prenantes ;
- l'analyse des données ;
- la préparation intellectuelle et la modération des différents ateliers ;
- la production des livrables provisoires et finaux.

6. Durée de la mission, calendrier des livrables et dispositions administratives

Le Consultant devra concevoir et fournir la supervision totale de la mission.

La mission se déroulera en 2023 avec au moins 3 déplacements en République Islamique de Mauritanie d'une durée suffisante pour permettre d'interagir avec les parties prenantes dans le cadre de ces termes de référence.

Il est prévu qu'elle débute le 1 juillet 2023.

La durée de la mission est de 16 semaines sans compter la période pour l'assistance à l'évaluation et suivi de la mise en œuvre qui aura lieu plus tard sur une période de 12 mois au maximum.

Le Consultant soumettra les livrables suivants selon le chronogramme indicatif ci-dessous :

Calendrier	**Livrables**	**Calendrier des paiement**
Signature du contrat + 1 semaine	• Rapport de lancement/cadrage et liste des parties prenantes nationales et régionales à inviter aux ateliers de consultation et de présentation du CSIRT et SOC et du programme de renforcement de capacités et de sensibilisation dans la cybersécurité	• 10% à la fourniture d'un rapport acceptable
Signature du contrat + 4 semaines	• Atelier de concertation avec les acteurs nationaux et régionaux	• 10% à la fourniture d'un rapport acceptable
Signature du contrat + 8 semaines	• Rapport d'évaluation de l'état de préparation / étude de faisabilité.	• 20% à la validation un rapport
Signature du contrat + 8 semaines	• Rapport d'audit de l'Intranet.	• 10% à la validation un rapport
Signature du contrat + 8 semaines	• Programme provisoire de renforcement de capacités et de sensibilisation	•
Signature du contrat + 10 semaines	• Cahier des charges pour la mise en place du CSIRT et du SOC et des interfaces et du Document d'appel d'offres et du système de filtrage des contenus.	• 10% à la validation un rapport
Signature du contrat + 11 semaines	• Atelier de présentation du rapport de faisabilité (Présentation PPTX, Actes de l'atelier)	• 10% à la fourniture du rapport de l'atelier
Signature du contrat + 12 semaines	• Tableau des effectifs du CSIRT et du SOC.	
Signature du contrat + 12 semaines	• Programme définitif de renforcement de capacités et de sensibilisation	
Signature du contrat + 14 semaines	• Plan d'affaires et catalogue de services	• 10% à la validation du rapport
Signature du contrat + 15 semaines	• Atelier de restitution du rapport final Plan de formation.	

Calendrier	Livrables	Calendrier des paiement
Signature du contrat + 16 semaines	• Rapport final incluant l'ensemble des rapports précédents et muni d'un résumé exécutif.	• 10% à la validation du rapport
Après le lancement de l'Appel d'offre	• Assistance à l'évaluation et suivi de la mise en œuvre (sur une période de 12 mois au maximum)	• 10% à la validation du rapport d'évaluation

Les autorités mauritaniennes assurent le Consultant de leur entière collaboration et mettent tout en œuvre afin que celui-ci obtienne – dans les délais les plus courts - toute information et tout document nécessaire à l'accomplissement de sa mission.

Le coût d'organisation des ateliers n'est pas à la charge du Consultant. Les autorités mauritaniennes assureront l'envoi des lettres d'invitation aux participants à l'atelier.

Le Consultant fournira tous les documents en français, en dix exemplaires papiers (impressions couleur de bonne qualité avec reliure de qualité) et une copie électronique (Word, Excel, PPTX, …).

Le Consultant partagera avec l'Unité de Gestion de Projet WARDIP, toute la documentation collectée durant la mission sur un répertoire partagé (exemple BOX).

Les différents rapports seront soumis à examen des autorités mauritaniennes de la Banque mondiale et devront inclure les remarques apportées jusqu'à leur entière satisfaction.

7. Aptitudes et qualification requises

Le Consultant doit être une firme ayant une expérience avérée dans les domaines objet de la mission. Le consultant doit se conformer à l'expérience et aux qualifications suivantes. Le consultant sera recruté sur une base concurrentielle conformément aux directives de passation des marchés de la Banque mondiale.

- Au moins 7 ans d'expérience en cybersécurité, en particulier la réponse aux incidents, le renseignement sur les cybermenaces, la criminalistique numérique et les SOC.
- Au moins 3 références de projets au cours des 5 dernières années d'évaluation, d'établissement / d'amélioration de CIRT / CSIRT / SOC nationaux / sectoriels. Des lettres de référence signées par le client doivent être fournies avec la proposition
- Au moins 3 références pour l'élaboration de programme de sensibilisation et de renforcement de capacités
- Au moins dix ans d'expérience avec :
    - Intégration et personnalisation des outils CSIRT/CERT/CIRT/SOC
    - Développer des politiques et des procédures liées aux opérations CSIRT/CERT/CIRT/SOC (flux de travail opérationnels, SOP, processus de gestion des incidents, cadres de gestion des niveaux de service, entre autres)

- Mise en place des outils du Cybersecurity Operation Center ; configuration des outils spécifiques et intégration des flux externes, mise en place des solutions d'investigation numérique

- Les projets antérieurs dans la région sont un plus

8. Qualifications de l'équipe du Consultant

L'équipe du consultant doit être composée d'au moins les membres suivants :

Chef d'équipe :

- Titulaire d'un diplôme Master universitaire ou ingénieur en informatique, TI, ingénierie ou domaine connexe ;
- Au moins dix (10) années d'expérience dans les programmes de cybersécurité ou la gestion de projet, en particulier la réponse aux incidents, le renseignement sur les cybermenaces et la criminalistique numérique.
- Une expérience avérée dans la gestion et la mise en œuvre de projets liés au CIRT/CERT/CSIRT/SOC dans les pays en développement serait un avantage
- Certifications pertinentes telles que CISSP, CISM ou GCIH et certification d'auditeur SOC reconnue internationalement
- Anglais courant

Membres de l'équipe de projet

- Au moins cinq ans d'expérience dans la cybersécurité, en particulier la réponse aux incidents, le renseignement sur les cybermenaces et la criminalistique numérique.
- Une expérience professionnelle avérée dans la mise en œuvre de projets liés au CIRT/CERT/CSIRT/SOC dans les pays en développement serait un avantage.
- Certifications pertinentes telles que CISSP, CISM ou GCIH et certification d'auditeur SOC reconnue internationalement
- Au moins un membre de l'équipe de projet doit être certifié EnCase Certified Examiner (EnCE) et/ou EnCase Certified eDiscovery Practitioner (EnCEP)
- Au moins un membre de l'équipe de projet doit être certifié Cellebrite Certified Mobile Examiner (CCME)
- Au moins un membre de l'équipe doit être certifié dans le domaine des Infrastructures Hyperconvergé et devra avoir une expérience dans la gestion des équipements réseaux, pares-feux physiques et applicatifs.
- Anglais courant

Expert en élaboration de plans de formation :

- Titulaire d'un diplôme BAC+5 ou supérieur en sciences de l'éducation, ingénierie pédagogique, cybersécurité ou dans un domaine connexe ;
- Avoir des certifications dans le domaine de la cybersécurité ;

- Au moins 10 ans d'expérience dans la conception, l'élaboration et la mise en œuvre de programmes de formation, notamment dans le domaine de la cybersécurité ;
- Expérience dans l'évaluation et l'amélioration des programmes de formation ;
- Excellente maîtrise du français et de l'anglais (écrit et oral).

Le Consultant pourra prévoir dans son équipe d'autres ressources d'appui.

La langue de travail à l'oral est le Français. Les livrables sont en Français.

Le Consultant pourrait être sollicité dans le cadre d'un avenant pour des prestations complémentaires.

9. Méthode de sélection

Le recrutement se fera suivant la méthode de sélection fondée sur la Qualification du Consultant (SQC) telle que décrite dans le Règlement de Passation des Marchés de la Banque Mondiale daté de juillet 2016, révisé en Novembre 2017, Août 2018 et Novembre 2020.

ANNEXE A – Parties prenantes à inclure dans les ateliers de consultation

- Les représentants des ministères et agences concernés ;
- Décideurs politiques et parlementaires intéressés ;
- Système judiciaire ;
- Organismes de réglementation ;
- Agences de sécurité nationale ;
- Etablissement de sécurité (ou ceux qui sont actuellement responsables de la sécurité de l'information et/ou de la gestion des technologies de l'information et des TIC) ;
- Les organismes d'application de la loi ;
- Fournisseurs d'infrastructures critiques (eau, énergie, transport, etc.) ;
- Banque centrale et banques (publiques et commerciales les plus pertinentes) ;
- Opérateurs de télécommunications et fournisseurs de services Internet ;
- Universités et les organismes nationaux de recherche ;
- Industrie locale (secteur privé) impliquée dans les initiatives de sécurité.

ANNEXE B - Bonnes pratiques reconnues pour la mise en place des CIRT

- Université Carnegie Mellon, 2016, Créer un CSIRT, Software Engineering Institute, Pittsburgh, PA. Cowley, C. et Pescatore, J., 2019, Pratiques courantes et meilleures pratiques pour les centres d'opérations de sécurité : résultats de l'enquête SOC 2019, SANS Institute. ENISA, 2006, Une approche étape par étape sur la façon de mettre en place un CSIRT. (https://www.enisa.europa.eu/publications/csirt-setting-up-guide)
- FIRST, 2019, Cadre de services de l'équipe de réponse aux incidents de sécurité informatique (CSIRT) (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1).
- IETF Internet Engineering Task Force, 1998, RFC 2350 pour les établissements CSIRT. (https://tools.ietf.org/html/rfc2350) ;
- Forum sur la gouvernance de l'Internet, 2014, Forum des meilleures pratiques sur la création et le soutien des équipes de réponse aux incidents de sécurité informatique (CSIRT) pour la sécurité Internet (https://www.intgovforum.org/multilingual/content/establishing-and-supporting-computer-incident-security -response-teams-csirts-for-internet).
- MITRE, 2014, Dix stratégies d'un centre d'opérations de cybersécurité de classe mondiale, MITRE, Bedford, MA.
- Morgus, R., Skierka, I., Hohmann, M. et Maurer, T., 2015, Les CSIRT nationaux et leur rôle dans la réponse aux incidents de sécurité informatique, New America et GPPi. (https://www.researchgate.net/publication/323358191_National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response)
- National Cyber Security Centre, 2015, CSIRT Maturity Kit, National Cyber Security Centre, La Haye.
- National Cyber Security Centre, 2017, Building a SOC: Start Small, National Cybersecurity Centre, La Haye.
- Organisation des États américains, 2016, Meilleures pratiques pour l'établissement d'un CSIRT national, OAS, Washington, DC
- Open CSIRT Foundation, 2008-2019, SIM3 : Modèle de maturité de la gestion des incidents de sécurité. (https://opencsirt.org/csirt-maturity/sim3-and-references/)

- Skierka, I., Morgus, R., Hohmann, M. et Maurer, T., 2015, CSIRT Basics for Policy-makers, New America et GPPi. (https://www.researchgate.net/publication/323358187_CSIRT_Basics_for_Policy-Makers)
- Secteur du développement des télécommunications (UIT-D), 2020, cadre ITU CIRT, Union internationale des télécommunications, Genève.
- ThaiCERT, 2017, Mise en place d'un CSIRT, équipe thaïlandaise d'intervention d'urgence informatique, Bangkok.
- TNO, 2017, Bonnes pratiques mondiales du GFCE : équipes nationales de réponse aux incidents de sécurité informatique (CSIRT). (https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf)