REPUBLIQUE DEMOCRATIQUE DU CONGO
PROJET D'APPUI A LA TRANSFORMATION NUMÉRIQUE EN RDC
(P180495)
ZR-CI-456518-CS-QCBS

TERMES DE REFERENCE D'UN CONSULTANT POUR L'ELABORATION DU CADRE STRATEGIQUE POUR LE DEVELOPPEMENT DE LA CYBERSECURITE EN RDC (ETUDE DE FAISABILITE ET PLAN DE MISE EN ŒUVRE D'ANCY, ELABORATION D'UN PLAN D'ACTION CYBERSECURITE, SPECIFICATIONS TECHNIQUES DU SYSTEME/EQUIPEMENT, EVALUATION CIRTS/SOC)

A. INTRODUCTION

Le Gouvernement de la RDC a obtenu une avance de fonds de la Banque mondiale pour financer les activités de préparation du Projet d'Appui à la Transformation Numérique de la RDC. Le projet devrait être mis en œuvre sur une période de cinq ans une fois qu'il sera entré en vigueur. Ces fonds serviront à financer les activités nécessaires à la maturation du projet et à faciliter sa mise en œuvre.

B. CONTEXTE ET OBJECTIFS DU PROJET

La RDC dispose d'un énorme potentiel dans le secteur numérique qui pourrait contribuer de manière significative au PIB du pays, augmenter les opportunités d'emploi et d'entrepreneuriat et améliorer la prestation de services à la population, mais ce potentiel n'est pas encore exploité.

Le taux de pénétration du haut débit s'élève actuellement à seulement 15,4 pour cent, sur la base d'abonnements à haut débit uniques[1] et les réseaux mobiles à large bande existants ne couvrent qu'environ la moitié de la population, avec des prix de détail du haut débit parmi les plus élevés d'Afrique. En outre, la prestation de services numériques est encore faible, avec peu de plateformes et de systèmes numérisés capables de faciliter l'efficacité des services publics et l'accès aux services par la population. La RDC manque également de compétences numériques et d'un écosystème d'innovation numérique pour soutenir la transformation numérique. Tous ces éléments, s'ils sont bien développés, peuvent contribuer et contribueront à créer d'immenses possibilités de création d'emploi, ainsi que de nombreuses possibilités d'entrepreneuriat pour les jeunes.

1. Description du Projet de Transformation Numérique de la RDC

Le Gouvernement de la RDC envisage de mettre en place un Projet de Transformation Numérique qui renforcera l'accroissement de l'accès à une connectivité haut débit abordable et de haute qualité, à des services et solutions numériques à fort impact et en demande, ainsi qu'à des compétences numériques pertinentes pour l'industrie. L'objectif de développement du projet est d'accroître l'accès et l'utilisation inclusifs de l'internet et renforcer les bases pour les services numériques en RDC.

Le projet proposé est conçu pour appuyer la transformation numérique du pays. Pour ce faire, il investira dans (i) l'infrastructure de connectivité numérique fondamentale nécessaire pour soutenir le mouvement vers l'accès numérique universel ; (ii) l'infrastructure publique numérique transversale (DPI) fondamentale requise pour faire évoluer les transactions numériques et à distance (dans les secteurs privé et public) ainsi que la prestation de services de manière rentable et sécurisée au niveau sectoriel ; (iii) le renforcement de la base de compétences numériques avancée et l'écosystème d'innovation numérique

[1] GSMA, 2022, Market Intelligence.

de la RDC pour garantir l'utilisation productive de la technologie, tout en créant des liens avec des emplois numériques et soutenir le développement de nouveaux services numériques, et (iv) le renforcement de la capacité institutionnelle et la gouvernance nécessaires pour mener des initiatives connexes de manière concertée et intégrée.

2. Les Composantes du Projet

Le Projet est constitué de cinq composantes réparties de la manière suivante :

Composante 1 - Élargir l'accès et l'inclusion numériques : Cette composante soutiendra le développement de cadres favorables et fournira un financement pour compléter et catalyser les investissements du secteur privé dans le déploiement d'infrastructures de réseaux à large bande, en vue d'accélérer les progrès de la RDC vers l'accès universel au haut débit et une inclusion numérique plus large, à travers l'extension du backbone fibre optique nationale et la connectivité rurale.

Composante 2 - Introduction de bases numériques pour la prestation de services : Cette composante soutiendra les investissements dans les éléments de base numériques transversaux nécessaires pour étendre de manière rentable et sécurisée la fourniture de services numériques à travers la RDC, en particulier du côté du secteur public, tout en soutenant leur intégration dans les services clés pour améliorer l'accès. Elle se concentrera sur les infrastructures et plates-formes numériques partagées et transversales qui permettraient au gouvernement d'étendre son utilisation aux outils numériques.

Composante 3 - Développer une main-d'œuvre compétente en matière de numérique et stimuler l'innovation dans les services numériques :
Cette composante soutiendra le développement des compétences numériques et du système national d'innovation, en améliorant les compétences et en renforçant les capacités des fonctionnaires, des étudiants et des entrepreneurs engagés dans des programmes dans le domaine de la technologie, en stimulant les liens entre le secteur de l'enseignement supérieur et le secteur technologique, et en alimentant le développement de solutions numériques locales qui encouragent une utilisation productive de la technologie numérique.

Composante 4 - Coordination institutionnelle et gestion du projet :
Cette composante financerait la gestion et la coordination du projet du bénéficiaire en matière de capacités, y compris la passation des marchés, la gestion financière, le suivi et l'évaluation, ainsi que la gestion des aspects environnementales et sociales (E&S).

Composante 5 - CERC : Cette composante est la composante d'intervention d'urgence (CERC).

3. Portée géographique du projet

Les activités du projet seront mises en œuvre à l'échelle nationale, en se concentrant principalement sur les 10 provinces du Cadre de partenariat pays (CPF) entre la Banque mondiale et le Gouvernement de la RDC, à savoir Kinshasa, Kwilu, Kongo-central, Kasaï, Kasaï-Central, Kasaï-Oriental, Lomami, Nord-Kivu, Sud-Kivu et Ituri ; ainsi que de nombreuses autres provinces à travers le pays.

4. Financement du projet

Le gouvernement de la RDC a obtenu une avance de préparation du projet (APP) à hauteur de 6 millions de dollars pour faciliter la préparation du projet, y compris la mise en place de la nouvelle Unité de Gestion du Projet (UGP). L'APP sera mise en œuvre par la Cellule d'Infrastructure, sous la tutelle du Ministère des Infrastructures et Travaux Publics. Toutefois, une nouvelle UGP sera créée au sein du Ministère des Postes, Télécommunications et Numérique (MPTN), qui gérera la mise en œuvre du projet principal. Le dispositif institutionnel se compose d'une série d'institutions qui jouent un rôle clé dans la mise en œuvre du projet et qui en sont également les bénéficiaires, dans le secteur numérique (MPTN, Ministère de l'Intérieur, le Ministère de l'Enseignement Supérieur et Universitaire, l'Agence pour le Développement du Numérique, Organisation Nationale pour l'Identification de la Population, L'Autorité de régulation de la poste et des télécommunications du Congo (ARPTC), Fond pour le développement de Service Universelle (FDSU), Société Congolaise de Fibre Optique (SOCOF, etc.)

Le projet principal est financé par la Banque mondiale pour montant de 400 millions de dollars et cofinancé par l'Agence Française de Développement (AFD) à hauteur de 100 millions d'euros. L'Accord de financement a été signé en novembre 2024, et sera mis en œuvre sur une période de 5 ans et se clôturera en décembre 2029.

Afin de soutenir les investissements prévus pour le développement des cadres de cybersécurité dans la composante 2 du projet, le projet souhaite recruter un consultant (firme) pour réaliser des études visant à identifier et mieux cartographier les besoins en cybersécurité dans le pays. Il s'agira de : i) effectuer une évaluation de la maturité de la cybersécurité nationale ; ii) définir un plan de mise en œuvre de la stratégie nationale de cybersécurité ; iii) définir un plan d'opérationnalisation de l'agence nationale de cybersécurité ; vi) réaliser une évaluation de l'état de préparation des réseaux de télécommunications et élaborer un plan de mise en œuvre des réseaux de télécommunications.

C. OBJECTIF DE LA MISSION

L'entreprise recrutée aura les objectifs suivants :

- Réaliser une évaluation de la maturité de la cybersécurité nationale, en identifiant les principales lacunes et en fournissant des recommandations prioritaires.
- Définir un plan de mise en œuvre qui traduise les objectifs de cybersécurité identifiés dans la Stratégie nationale de cybersécurité en une approche progressive et budgétisée, adaptée à la RDC.
- Définir un plan pour opérationnaliser l'Agence Nationale de Cybersécurité (ANCY), dans le but d'informer et conseiller le Gouvernement de la RDC sur l'opérationnalisation organisationnelle, fonctionnelle et technique de l'ANCY.
- Réaliser une évaluation de l'état de préparation du CIRT et développer un plan d'établissement du CIRT (« le Plan »). Le Plan reflétera les besoins, exigences et objectifs du pays et détaillera les services que le CIRT national devrait fournir, son public cible et les ressources nécessaires. Le Plan devrait également inclure une feuille de route étape par étape pour établir un CIRT national, ainsi que les documents d'appel d'offres pertinents. Le Consultant intégrera les Bonnes Pratiques largement acceptées pour permettre au CIRT national, établi à travers le Plan, de participer aux initiatives et forums de coopération internationale (par exemple, FIRST).
- Préparer un plan de renforcement des capacités pour le développement de la cybersécurité en RDC (y compris les cyber-analystes et les cyber-professionnels) ainsi que prérequis
- Elaborer de DAOs pour les différents systèmes et équipements.

Le périmètre des services, les profils de l'équipe de consultants, les exigences de reporting et d'autres particularités de la mission sont détaillés ci-dessous.

D. TACHES ET PRESTATIONS DU CONSULTANT

Le Consultant adoptera une approche par phases, en s'appuyant sur des cadres méthodologiques reconnus internationalement (notamment le Cyber Maturity Model (CMM), le Guide pour développer une stratégie nationale de cybersécurité, NIST, NCRA, IRAM2, évaluation de la préparation du CIRT par l'UIT, établissement de CSIRT par l'ENISA, etc.). Plus précisément, le Consultant est censé réaliser les activités suivantes :

1. **Réaliser une évaluation approfondie de la maturité de la cybersécurité nationale :**
    a) Élaborer un plan détaillé pour mener à bien la mission, y compris l'approche et la méthodologie proposées basées sur des cadres reconnus internationalement.
    b) Préparer toutes les informations logistiques pertinentes et les exigences pour les processus de consultation des parties prenantes et de collecte de données, y compris les modèles d'engagement des parties prenantes, une liste des organisations idéales pour participer aux ateliers, les installations nécessaires, etc.
    c) Avec le soutien du Ministère du de Poste, Télécommunications et Numérique, l'ADN et les instances appropriées au sein du gouvernement et à la Présidence chargé de la cyber sécurité, identifier et établir toutes les parties prenantes concernées par les enjeux de cybersécurité en RDC, leurs rôles et celles qui participeront au processus de consultation.
    d) Mener des recherches documentaires contextuelles, basées sur la littérature disponible publiquement et les documents pertinents partagés par le gouvernement, pour comprendre le contexte de la cybersécurité du pays. Préparer des demandes de données, telles que des questionnaires ou des questions d'entretien, à utiliser lors des consultations des parties prenantes et de la collecte de données.
    e) En étroite collaboration avec le gouvernement et avec leur soutien, organiser une session ou atelier de consultation avec les principales parties prenantes des secteurs public et privé, de la société civile et du monde académique. Rassembler toutes les données nécessaires pour l'analyse et l'examen des risques et des capacités de cybersécurité du pays.
    f) Mettre en œuvre toutes les mesures de contrôle de qualité possibles pour garantir la qualité, la fiabilité et la validité des données collectées lors de l'atelier de consultation des parties prenantes. Combler les lacunes potentielles qui auraient pu surgir lors du processus de collecte de données sur place grâce à des recherches documentaires supplémentaires ou à des sessions de suivi à distance avec les parties prenantes.
    g) Identifier les besoins et les lacunes en matière de renforcement des capacités du gouvernement de la RDC à améliorer la cybersécurité, et proposer une structure ou un modèle pour les formations requises sur la base des analyses pour les différents niveaux/catégories de bénéficiaires et/ou d'agents publics ou du secteur privé ou des jeunes.
    h) Analyser les informations collectées et produire un rapport préliminaire, en fournissant des recommandations évaluées par les pairs qui permettront à la RDC de renforcer sa capacité en matière de cybersécurité et sa compétence dans la gestion des risques liés à la cybersécurité.
    i) Présenter et valider les conclusions et les recommandations du rapport avec les parties prenantes nationales concernées.
    j) Produire une version finale du rapport qui intègre les retours reçus et soumettre les rapports finaux au gouvernement.

2. **Développer un plan d'action pour la mise en œuvre de la Stratégie nationale de cybersécurité :**
   a) Sur la base de l'évaluation de la maturité, de la Stratégie nationale de cybersécurité et du processus de consultation des parties prenantes, identifier les priorités et les objectifs stratégiques de la RDC.
   b) Élaborer un plan d'action basé sur les priorités et les objectifs stratégiques énoncés dans la Stratégie nationale de cybersécurité. Ce plan inclura des actions prioritaires, phasées, budgétées et attribuables visant à mettre en œuvre et à opérationnaliser la stratégie.
   c) Consulter les parties prenantes concernées pour valider le document et élaborer la version finale du plan d'action pour approbation par le gouvernement.
   d) Préparer jusqu'à 6 termes de référence (y compris les spécifications techniques et la documentation préliminaire des 'appel d'offres nécessaires) pour les activités de cybersécurité pertinentes incluses dans le plan d'action, notamment mais sans s'y limiter : le développement d'un cadre de protection des infrastructures critiques ; le développement et la mise en œuvre d'un programme de protection des services de gouvernance électronique ; le développement des capacités de réponse aux incidents ; la sensibilisation et le développement des compétences en cybersécurité ; l'harmonisation du cadre juridique de la cybersécurité et de la protection des données avec les bonnes pratiques régionales et internationales, etc.

3. **Définir un plan pour opérationnaliser l'agence nationale de cybersécurité :**
   a) Réaliser une analyse détaillée du cadre de gouvernance actuel de la cybersécurité du pays. Les données et documents pertinents peuvent être collectés à travers des consultations avec les parties prenantes, demandés au gouvernement ou consultés par des recherches documentaires si disponibles.
   b) Examiner le cadre juridique et réglementaire récemment promulgué pour identifier le mandat, les exigences, les rôles et les responsabilités de l'ANCY.
   c) Élaborer un plan détaillé pour l'établissement de l'agence, décrivant la structure organisationnelle, les besoins en personnel et la typologie de postes requis (y compris le qualifications requises), les estimations budgétaires, les mécanismes de financement et un calendrier de mise en œuvre.
   d) Elaborer le projet de manuelle stratégique et le manuel de procédures de l'Agence, pour la validation par le gouvernement.
   e) Fournir des recommandations sur les mécanismes de gouvernance et de coordination qui doivent être établis pour assurer le bon fonctionnement de l'agence (en interne et en externe, en fonction des cadres juridiques applicables). Cela inclut les mécanismes de collaboration inter-agences et internationales.
   f) Offrir des conseils sur les changements légaux, politiques et réglementaires nécessaires pour soutenir le mandat de l'agence.
   g) Évaluer les besoins en formation et en renforcement des capacités pour le personnel de l'agence.
   h) Rédiger les termes de référence et la documentation pertinente pour les appels d'offres.

4. **Développer un plan d'établissement du CIRT.**
   a) Préparer l'évaluation sur site : Le consultant réalisera des études et des analyses des capacités actuelles de réponse aux incidents du pays ainsi que de l'état général de la cybersécurité. Les données et documents pertinents peuvent être demandés au gouvernement ou consultés par des recherches documentaires si disponibles. Cette tâche inclut la préparation d'une liste des parties prenantes pertinentes à interviewer lors des ateliers de consultation.

b) Organiser des sessions ou réunions de consultation avec les parties prenantes nationales et régionales pertinentes : le consultant tiendra une série d'interactions et de discussions avec les parties prenantes concernées pour évaluer le niveau de préparation à la création d'un CIRT national. Dans cette activité, le consultant mènera des entretiens, recueillera des besoins et discutera des lacunes existantes et des remédiations possibles. Cette tâche informera les tâches 4.3 et 4.4.

c) Rédiger le rapport d'évaluation de l'état de préparation : le consultant préparera un rapport basé sur les informations collectées dans les tâches 1 et 2. Le rapport fournira un aperçu des capacités de réponse aux incidents existantes dans le pays, décrira les exigences préliminaires (par exemple, mandat, gouvernance, feuille de route à haut niveau, budget) pour le plan d'établissement du CIRT, et fournira des informations sur le contexte plus large de la cybersécurité. Ce rapport inclura notamment :
   i. Une brève revue des capacités de réponse aux incidents existantes
   ii. Un mandat préliminaire
   iii. Une structure de sa gouvernance
   iv. Les exigences pour l'organisation hôte du CIRT
   v. Une feuille de route et un budget à haut niveau
   vi. Les exigences à haut niveau pour la phase de conception

d) Rédiger le plan d'établissement du CIRT : le consultant développera un plan complet qui définit les services, le public cible, les ressources nécessaires et d'autres éléments pertinents pour établir un CIRT national dans le pays. Le consultant fournira également une feuille de route étape par étape pour la mise en œuvre du plan. Le plan inclura notamment :
   i. Un mandat détaillé
   ii. Un plan des services du CIRT
   iii. Un plan des processus et flux de travail du CIRT
   iv. Un plan de l'organisation, des compétences et de la formation du CIRT
   v. Un plan des installations du CIRT
   vi. Un plan des technologies et de l'automatisation des processus du CIRT
   vii. Un plan de coopération du CIRT
   viii. Un plan de gestion de la sécurité informatique et de l'information du CIRT
   ix. Une feuille de route détaillée et des exigences pour la phase de mise en œuvre
   x. Les documents d'appel d'offres pour contracter des consultants pour la mise en œuvre du plan.

5. Organiser un atelier pour présenter les livrables et sensibiliser les parties prenantes concernées :

a) Développer des supports digestes pour présenter les livrables de cette mission.
b) Présenter les livrables aux parties prenantes concernées.
c) Animer des discussions et des sessions de partage d'expérience, ainsi que des discussions interactives pour encourager l'apprentissage collaboratif.
d) Dispenser une session de sensibilisation à la cybersécurité aux fonctionnaires gouvernementaux.

E. LIVRABLES ET CALENDRIER DE RÉALISATION

Le Consultant est tenu de mener à bien la mission dans son intégralité en 24 semaines, et de soumettre les livrables suivants, sur la base des délais indicatifs et du calendrier de paiement détaillés ci-dessous

S/No	Livrable	Calendrier	Paiement indicatif
L1.	**Rapport de démarrage,** détaillant comment la mission sera réalisée, jugé acceptable par le Client	Dans une semaine après la signature du contrat	10%
L2.	**Évaluation de la maturité de la cybersécurité nationale,** conformément à l'activité 1	10 semaines, après la signature du contrat	30%
L3.	**Plan d'action pour la mise en œuvre de la Stratégie nationale de cybersécurité,** conformément à l'activité 2	12 semaines, après la signature du contrat	
L4.	**Plan pour opérationnaliser l'agence nationale de cybersécurité (ANCY),** conformément à l'activité 3	16 semaines, après la signature du contrat	35%
L5.	**Rapport d'évaluation de l'état de préparation & plan d'établissement du CIRT,** conformément à l'activité 4	18 semaines, après la signature du contrat	
L6.	**Termes de référence et documentation d'appel d'offres,** conformément aux activités 2, 3 et 4	19 semaines, après la signature du contrat	
L7.	**Atelier de validation,** conformément à l'activité 5	22 semaines, après la signature du contrat	
L8.	**Rapport final**	24 semaines, après la signature du contrat	25%

F. RESPONSABILITE DU CONSULTANT

Dans sa proposition, le consultant décrira l'approche qu'il compte adopter pour réaliser cette mission. En outre, il précisera les méthodes de travail et les moyens retenus pour la réalisation de ce mandat.

Pour chacun des objectifs, le consultant définira les activités qui mèneront aux résultats visés. Il intégrera un calendrier ou un plan d'actions pour chaque phase de la mission identifiée ci-dessus.

Le Consultant soumettra tous les livrables au Coordonnateur de la Cellule Infrastructures ou à l'UGP du PATN pour leur validation par les institutions et agences concernées. Les livrables écrits doivent être transmis électroniquement en format PDF et Word modifiable, pour y insérer des commentaires et des corrections.

Le Consultant est censé travailler quotidiennement avec le Spécialiste PIU désigné par le Gouvernement, ainsi qu'avec le point focal de l'ANCY qui sera le principal bénéficiaire de cette mission.

G. RESPONSABILITÉS DU CLIENT

Sous la coordination de la Cellule Infrastructures ou de l'UGP du PATN, les agences concernées de la présidence et du Ministère des Postes, Télécommunications et Numérique fourniront, dans la mesure de leurs possibilités :

- Toutes les données de fond et la littérature considérées comme pertinentes pour accomplir ou informer la mission et compléter les tâches identifiées à leur disposition immédiate.
- Accès aux principaux responsables au sein des ministères/agences/départements pertinents et autres entités officielles pertinentes, le cas échéant.
- Faciliter la coopération avec d'autres organisations dont les activités et programmes peuvent être considérés comme pertinents pour la mission.
- Accompagner les consultants lors des réunions consultatives et soutenir l'organisation des ateliers pertinents.

H. LIEU

La firme sélectionnée doit être disponible pour travailler en RDC (par exemple, à travers des missions sur le terrain) afin de faciliter la collecte des données nécessaires, de comprendre le contexte local et de favoriser un transfert de connaissances plus efficace.

I. TRANSFERT DE CONNAISSANCES

Le transfert de connaissances est considéré comme une partie intégrante de cette mission et doit être reflété dans la méthodologie du consultant et la proposition technique. Idéalement, le gouvernement devrait être en mesure d'apprendre comment reproduire / mettre à jour les éléments clés de la mission, si nécessaire, à l'avenir.

J. CONSULTATION DES PARTIES PRENANTES

Le Consultant est censé s'engager dans une consultation des parties prenantes pour mener à bien la mission, qui doit être documentée et partagée avec l'Unité de Gestion du Projet (UGP).

K. PROFIL ET QUALIFICATIONS

L'entreprise sélectionnée devra démontrer :

- Au moins cinq (5) ans des compétences solides et une expérience en cybersécurité et en technologies de l'information et de la communication (TIC), notamment dans les domaines suivants : gouvernance et législation, gestion des risques, protection des infrastructures d'information critiques, réponse aux incidents, renseignement sur les menaces cybernétiques et criminalistique numérique, et développement des compétences en cybersécurité, avec au moins 5 ans d'expérience pertinente.
- La conduite d'au moins trois (3) projets de conception et de mise en œuvre des politiques, stratégies et opérations de cybersécurité dans un contexte gouvernemental.
- Une méthodologie appropriée et une expérience de l'application d'outils de recherche connexes.
- Avoir réalisé au moins trois (3) missions de développement de politiques/gouvernance en cybersécurité, de préférence dans des contextes en développement (L'un d'entre eux devrait se trouver dans un pays africain)
- Avoir réalisé au moins trois (3) évaluations/établissements de CIRT ou des missions similaires, de préférence dans des contextes en développement.

- Une compréhension des cadres, méthodologies et meilleures pratiques clés en cybersécurité (y compris : Guide pour le développement d'une stratégie nationale de cybersécurité, CMM (Capability Maturity Model), NIST CSF, ISO 2700x, etc.) et en réponse aux incidents.
- Une expérience préalable de travail avec le secteur public est préférée.
- Une expérience dans un contexte de pays en développement est considérée comme un avantage.
- Bonne connaissance et compréhension du secteur numérique en Afrique
- Bonne connaissance et expérience de la collaboration avec les gouvernements des pays en développement (une expérience en Afrique est un atout)
- Capacité à réaliser la mission en français.

L'entreprise doit proposer au moins une équipe avec les profils ci-dessous, ainsi que tout personnel de soutien supplémentaire jugé nécessaire pour mener à bien la mission. Tous les membres de l'équipe doivent parler couramment l'anglais et être capables de réaliser la mission en français.

L'entreprise de conseil doit fournir un plan de dotation en personnel avec les noms, rôles et CV de l'équipe de projet de base dans le cadre de la proposition.

Personnel clé	Expérience	Qualifications
Un (1) Chef équipe	• Minimum 7 ans d'expérience dans l'industrie de la cybersécurité. • Cinq (5) ans d'expérience dans la conduite de projets de cybersécurité et connaissance des meilleures pratiques mondiales en matière de développement de politiques de cybersécurité. • Excellentes compétences en communication et en leadership, et expérience dans la gestion de projets complexes. • Expérience antérieure en réseautage et collaboration avec des institutions gouvernementales.	• BAC + 5 ou master en informatique, cybersécurité, sciences/technologies et/ou autres domaines équivalents. • Maîtrise du français requise.
Un (1) Expert en gouvernance juridique de la cybersécurité	• Au moins 5 ans d'expérience en gouvernance et aspects juridiques de la cybersécurité, avec un accent sur les politiques et réglementations nationales. • Conduite d'au moins deux (2) projets les cinq (5) dernières années de conception et de mise en œuvre des politiques et réglementations de cybersécurité conformément aux normes et réglementations nationales et internationales pertinentes. • Connaissance des exigences légales et réglementaires pertinentes, telles que les réglementations sur la protection des données, la législation sur l'utilisation abusive des ordinateurs et les politiques de protection des infrastructures critiques.	• BAC + 5 ou master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, droit, sciences/technologies ou autres domaines équivalents.

Un (1) Spécialiste de la gestion des risques et de la CIIP	• Au moins 5 ans d'expérience en gestion des risques et CIIP, de préférence au niveau national. • Connaissance approfondie des cadres de gestion des risques et CIIP, tels que NIST SP 800-53, ISO/IEC 27001 ou CIP-014-1, et leur application aux processus de protection des IIC. • Certifications pertinentes, telles que Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) ou Certified Critical Infrastructure Protection Professional (CCIPP), fortement souhaitées.	• BAC + 5 ou master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, sciences/technologies ou autres domaines équivalents.
Deux (2) Spécialistes de la réponse aux incidents	• Au moins 5 ans d'expérience en réponse aux incidents de cybersécurité, avec un accent sur l'établissement et la gestion des CIRTs. • Connaissance approfondie des cadres et méthodologies de réponse aux incidents et d'établissement de CIRT, tels que le cadre de services FIRST, NIST SP 800-61, ISO/IEC 27035, les directives de gestion des incidents de SANS, et leur application à la construction et à l'exploitation de CIRTs efficaces. • Conduite d'au moins deux (2) projets les cinq (5) dernières années, de conception et de mise en œuvre des politiques, procédures et flux de travail de réponse aux incidents, et de formation et d'encadrement des membres du CIRT sur les meilleures pratiques de réponse aux incidents. • Trois (3) ans d'expérience antérieure dans l'établissement de CIRT. • Certifications pertinentes, telles que Certified Information Systems Security Professional (CISSP), GIAC Certified Incident Handler (GCIH) ou EC-Council Certified Incident Handler (ECIH), fortement souhaitées.	• BAC + 5 ou master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, sciences/technologies ou autres domaines équivalents.
Un (1) Spécialiste du développement des compétences en cybersécurité	• Au moins 5 ans d'expérience dans le développement des compétences en cybersécurité. • Au moins 2 ans d'expérience à concevoir et dispenser des programmes de formation en cybersécurité, y compris le développement de programmes, la conception pédagogique et la prestation de cours. • Au moins 2 ans d'expérience d'utilisation de divers outils et techniques de formation en cybersécurité, tels que les simulations, les exercices pratiques et les plateformes de formation en ligne.	• BAC + 5 ou master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, sciences/technologies ou autres domaines équivalents.

ANNEX A- Recognized good practices for establishing CIRTs

- Carnegie Mellon University, 2016, Create a CSIRT, Software Engineering Institute, Pittsburgh, PA. Cowley, C. and Pescatore, J., 2019, Common and best practices for security operations centers: Results of the 2019 SOC survey, SANS Institute. ENISA, 2006, A step-by-step approach on how to set up a CSIRT. (https://www.enisa.europa.eu/publications/csirt-setting-up-guide)
- FIRST, 2019, Computer Security Incident Response Team (CSIRT) Services Framework (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1).
- IETF Internet Engineering Task Force, 1998, RFC 2350 for CSIRT establishments. (https://tools.ietf.org/html/rfc2350)
- Internet Governance Forum, 2014, Best practice forum on establishing and supporting computer security incident response teams (CSIRTs) for internet security (https://www.intgovforum.org/multilingual/content/establishing-and-supporting-computer-incident-security-response-teams-csirts-for-internet).
- MITRE, 2014, Ten strategies of a world-class cybersecurity operations center, MITRE, Bedford, MA.
- Morgus, R., Skierka, I., Hohmann, M. and Maurer, T., 2015, National CSIRTs and their role in computer security incident response, New America and 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, the Hague.
- National Cyber Security Centre, 2017, Building a SOC: Start Small, National Cybersecurity Centre, the Hague.
- Organization of American States, 2016, Best Practices for Establishing a National CSIRT, OAS, Washington, D.C.
- Open CSIRT Foundation, 2008-2019, SIM3: Security Incident Management Maturity Model. (https://opencsirt.org/csirt-maturity/sim3-and-references/)
- Skierka, I., Morgus, R., Hohmann, M. and Maurer, T., 2015, CSIRT Basics for Policy-makers, New America and GPPi. (https://www.researchgate.net/publication/323358187_CSIRT_Basics_for_Policy-Makers)
- Telecommunications Development Sector (ITU-D), 2020, ITU CIRT framework, International Telecommunication Union, Geneva.
- ThaiCERT, 2017, Establishing a CSIRT, Thailand Computer Emergency Response Team, Bangkok.
- TNO, 2017, GFCE global good practices: National computer security incident response teams (CSIRTs). (https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf)