REPUBLIQUE DU BURUNDI

MINISTERE DE LA COMMUNICATION, DES TECHNOLOGIES DE L'INFORMATION ET DES MEDIAS (MINCOTIM).

PROJET D'APPUI AUX FONDATIONS DE L'ECONOMIE NUMERIQUE (PAFEN)

(P176396).

TERMES DE REFERENCE

BUREAU D'ETUDES POUR LA CYBERSECURITE : ASSISTANCE TECHNIQUE DE LA « COMMISSION CHARGEE DE L'ELABORATION DE LA STRATEGIE NATIONALE SUR LA CYBERCRIMINALITE ET LA CYBERSECURITE ».

JUIN 2023

I. PREAMBULE

Le Gouvernement du Burundi a obtenu un don de la Banque mondiale pour financer le « Projet d'Appui aux Fondations de l'Economie Numérique » (PAFEN) en sigle, ou « Burundi Digital Foundations Project » en anglais.). Il est prévu qu'une partie des ressources allouée à ce projet soit utilisée pour financer des prestations d'un bureau d'études pour l'assistance technique de la « commission chargée de l'élaboration de la stratégie nationale sur la cybersécurité et la cybercriminalité ».

II. CONTEXTE ET OBJECTIFS DU PROJET

L'objectif de développement du Projet d'Appui aux Fondations de l'Economie Numérique (PAFEN) est d'augmenter l'accès à l'internet à haut débit, en particulier pour les populations mal desservies ; et améliorer la capacité du Gouvernement à fournir des services publics par voie numérique.

Le projet vise à accroître l'accès au haut débit et à améliorer la capacité du gouvernement à fournir des services publics numériques, ce qui contribuera à jeter les bases d'un développement accéléré de l'économie numérique du Burundi.

A. Les Composantes du Projet

Le Projet comprend 4 composantes ci-après :

Composante 1 : Accès et inclusion numériques

- Sous-composante 1.1 : Environnement favorable au développement du marché du haut débit et à l'accès numérique
- Sous -composante 1.2 : Accès à la connectivité locale
- Sous -composante 1.3 : Facilitateurs d'accès local et d'inclusion numérique

Composante 2 : Facilitateurs de la prestation de services publics numériques

- Sous-composante 2.1 : Cadres institutionnels, juridiques, de gouvernance et technologiques pour les services en ligne
- Sous -composante 2.2 : Infrastructure et plates-formes gouvernementales numériques partagées
- Sous -composante 2.3 : Numérisation de certains services et de cas d'utilisation phares

Composante 3 : Coordination institutionnelle et gestion du projet.

Composante 4 : Composante de réponse d'urgence (CERC)

Le PAFEN soutiendra une série de réformes visant à rapprocher les services des citoyens et à améliorer l'efficacité et la transparence du secteur public. De plus, le projet vise à soutenir l'utilisation des technologies numériques et des données pour faciliter la prise de décisions politiques et promouvoir les investissements.

La Politique Nationale de Développement des Technologies de l'Information et de la Communication *(*PNDTIC) du gouvernement du Burundi a identifié les réformes de l'économie numérique et la numérisation du secteur public comme des priorités politiques essentielles pour le pays, au moment où le cadre politique, juridique et réglementaire reste incomplet.

Les infrastructures et systèmes de communication et de traitement de l'information sont de plus en plus exposés aux nouvelles formes d'activités illégales (infections virales, mises hors service, actes d'intrusion, usurpations d'identité, vols d'information, menaces diverses sur les personnes, chantages, divulgation de secrets personnels, etc.).

En effet, la prolifération des services fournis et les différents modes d'accès aux technologies de l'information et de la communication (TIC) ont fait émerger de nouveaux risques menaçant la sécurité des équipements et des données avec des conséquences, tant sur les biens que sur la vie privée des personnes.

La multiplication et la complexité croissante des actions malveillantes, tout comme l'ampleur des dégâts potentiels mettent en évidence la nécessité d'une réponse adéquate et efficace à ces risques.

Tous les pays sont confrontés à la problématique de la nécessité de faire partie de la Société de l'Information, en prenant en considération le risque de leur dépendance vis-à-vis de ces technologies et sans perdre de vue que la fracture digitale existante ne doit pas se doubler d'une fracture sécuritaire, encore moins d'une dépendance plus forte d'entités qui contrôleraient leurs besoins et moyens de sécurité des technologies de l'information.

La sécurité est la pierre angulaire de toute activité dans le cyberespace et doit être vue comme un service créant un cadre de confiance permettant la création et l'utilisation d'autres services (e-gouvernement, e-santé, e-éducation, transactions électroniques, etc.). La sécurité informationnelle touche à la sécurité du patrimoine numérique des organisations publiques et privées, ainsi qu'à la vie privée et aux biens des individus. Elle constitue de nos jours, un enjeu de premier ordre dont la satisfaction passe par des actions politiques notamment la définition d'une Stratégie Nationale de Cybersécurité cohérente, inclusive et efficace.

Cette stratégie devrait nécessiter le renforcement au niveau national, de capacités de réaction appropriées pour faire face aux incidents opérationnels de cybersécurité, et en particulier par l'opérationnalisation des équipes d'intervention en cas d'incident informatique (CERT). A noter à cet effet les actions que le Burundi a entrepris avec l'UIT pour la mise en place du CERT.

B. Besoin de la stratégie nationale de cybersécurité

Une stratégie nationale de cybersécurité doit s'inscrire dans une approche pluridisciplinaire et apporter une réponse adéquate aux aspects politiques, techniques, juridiques, institutionnels et pédagogiques du phénomène.

Au Burundi, le besoin de disposer d'un cadre de référence en matière de sécurité des systèmes d'information et des transactions électroniques est devenu un besoin essentiel, et il est désormais urgent de :

- Mettre en place un cadre légal approprié ;
- Mettre en place un cadre institutionnel adéquat ;
- Promouvoir et sensibiliser les acteurs de la Société de l'Information à la sécurité des systèmes d'information.

Aussi, aux termes de la Convention de l'Union Africaine sur la Cybersécurité et la Protection des Données à Caractère Personnel, adoptée en 2014, les Etats signataires, se sont engagés, en collaboration avec toutes les parties prenantes, à se doter d'une politique nationale de cybersécurité qui reconnaît l'importance de l'infrastructure essentielle de l'information pour les Etats. Sur le plan international, la sécurité du Cyberespace préoccupe toutes les nations. L'Organisation des Nations Unies a pris à bras le corps la question en adoptant plusieurs résolutions depuis 2001.

Dans la Résolution N°58/199 adoptée par l'Assemblée Générale le 30 Janvier 2004, l'ONU invite les Etats membres à prendre en compte, entre autres, les éléments annexés à ladite Résolution, dans l'élaboration de leur stratégie de réduction de risques pour les infrastructures critiques, conformément à leurs législations nationales.

Il est un devoir pour les pouvoirs publics de mettre en place des politiques et stratégies de prévention, de protection et de défense des systèmes d'informations des organismes publics et privés et de sensibiliser les entreprises et les citoyens sur les enjeux et les risques liés aux menaces informatiques. La lutte contre la cybercriminalité ne peut être efficace que dans un

cadre de coopération internationale, compte tenu de la nature transnationale de cette forme de délinquance qui se passe des contraintes transfrontalières. La coopération entre les organes de répression et les fournisseurs d'accès aux services de télécommunications et internet est plus qu'indispensable, afin de favoriser les échanges d'information et la communication des données du trafic stockées. Tout cela n'est possible que si, les Etats disposent d'un minimum de standard sécuritaire.

C'est ainsi que le Gouvernement de la République du Burundi a mis en place, par ordonnance ministérielle n°580/08 du 26 novembre 2020, la « **Commission chargée de l'Elaboration de la Stratégie Nationale sur la Cybersécurité et la Cybercriminalité** » avec pour mission de :

- Faire l'analyse sur l'Etat des lieux de la Cybersécurité et des cyber risques au Burundi
- Elaborer une Stratégie nationale sur la Cybersécurité et la Cybercriminalité au Burundi ainsi qu'un plan d'actions de sa mise en œuvre.

Le PAFEN prévoit de recruter une assistance technique pour appuyer cette commission dans le processus de réalisation de toutes ses missions lui assignées par le gouvernement, afin que les travaux de la Commission soient non seulement professionnels mais aussi que les résultats attendus se conforment aux normes internationales en matière de Cybersécurité.

III. OBJECTIF GENERAL DE LA MISSION

Le Gouvernement du Burundi recherche les services d'une entreprise qualifiée (le « consultant ») pour conduire une l'évaluation du risque et de la capacité nationale en matière de cybersécurité et, sur la base de cette évaluation, pour développer une Stratégie Nationale sur la Cybersécurité et la Cybercriminalité comprenant un plan d'actions pour sa mise en œuvre, ainsi qu'une architecture institutionnelle pour la gestion de la cybersécurité au niveau national. L'étendue des services, les profils de l'équipe de consultants, les exigences en matière de rapport et autres détails de la mission sont détaillés ci-dessous.

IV. ETENDU DE LA MISSION

La mission du Consultant (Cabinet/Conseil) est de conduire une 'évaluation du risque et de la capacité nationale en matière de cybersécurité ; élaborer une Stratégie Nationale sur la Cybersécurité et la Cybercriminalité ; élaborer un plan d'actions pour sa mise en œuvre ; élaborer l'architecture institutionnelle pour la gestion de la cybersécurité au niveau national ; et présenter les livrables aux parties prenantes nationales concernées lors d'un atelier dédié.

En particulier, le Consultant est censé effectuer les tâches suivantes : l'

1 Réaliser une évaluation approfondie du risque et de la capacité nationale en matière de cybersécurité selon des cadres méthodologiques reconnues à niveau international, notamment NIST, NCRA, COBIT etc pour l'analyse du risque ; et le Cyber Maturity Model (CMM) du Global Cyber Security Capacity Centre pour l'évaluation de la capacité. Pour cette tache le Consultant devra :

- Élaborer un plan détaillé pour mener à bien la mission, y compris l'approche proposée et la méthodologie basée sur le cadre méthodique CMM ;
- Élaborer toutes les informations logistiques pertinentes et les exigences nécessaires pour la consultation des parties prenantes et le processus de collecte de données, y compris les modèles d'engagement des parties prenantes, la liste des organismes idéaux pour participer aux ateliers, les installations nécessaires, etc ;
- Avec le soutien du MINCOTIM, identifier toutes les parties prenantes pertinentes qui participeront au processus de consultation ;
- Réaliser une recherche documentaire contextualisée en s'appuyant sur la littérature publiquement disponible, ainsi que sur les documents pertinents partagés par le gouvernement, afin de comprendre le contexte du pays ; et préparer des demandes de données, qui pourraient prendre la forme de questionnaires ou de questions d'entretien, à utiliser lors de la consultation des parties prenantes et du processus de collecte de données ;
- En étroite collaboration avec le MINCOTIM et en facilitant leur soutien, organiser un atelier de consultation de cinq jours avec les principales parties prenantes des secteurs public et privé, de la société civile et du milieu universitaire, et recueillir toutes les données nécessaires pour l'analyse et l'examen du risque et de la capacite nationale en matière de cybersécurité ;
- Mettre en œuvre toutes les mesures possibles de contrôle qualité afin d'assurer la qualité, la fiabilité et la validité des données collectées lors de l'atelier de consultation des parties prenantes. Combler les éventuelles lacunes qui ont pu apparaître lors du processus de collecte de données sur place en effectuant des recherches documentaires ultérieures ou en organisant des sessions de suivi à distance avec les parties prenantes ;
- Analyser les informations collectées et produire un projet de rapport CMM ainsi qu'un rapport d'évaluation des risques, en fournissant des recommandations évaluées par des

pairs qui permettront au Burundi de renforcer sa capacité en matière de cybersécurité et sa compétence dans la gestion des risques liés à la cybersécurité ;

- Faciliter un atelier de validation pour présenter et valider les conclusions et les recommandations issues du projet de rapport CMM et du rapport d'évaluation des risques ;
- Produire les rapports finaux CMM et d'évaluation des risques qui reflètent/incorporent les commentaires de l'atelier de validation, et soumettre les rapports finaux au gouvernement.

2 Elaborer un modèle d'architecture institutionnelle pour la gestion de la cybersécurité qui définit les rôles et responsabilités au niveau national. Pour cette tâche le Consultant doit se baser sur le CMM au point 1 et devra :

- Réaliser une analyse préliminaire pour identifier les institutions et organismes impliqués dans la gestion de la cybersécurité, évaluer leurs capacités actuelles et identifier les besoins pour l'architecture institutionnelle ;
- Effectuer une étude comparative pour examiner les modèles institutionnels adoptés par d'autres pays, analyser leurs forces, faiblesses et bonnes pratiques, et identifier les éléments pertinents pour le contexte national au Burundi ;
- Organiser des réunions et des ateliers de consultation avec les parties prenantes clés, recueillir leurs opinions et recommandations, et favoriser la collaboration pour parvenir à un consensus ;
- Sur la base de l'analyse, étude comparative et consultation avec les parties prenantes, proposer et valider une structure institutionnelle adéquate pour la gestion de la cybersécurité, établir des mécanismes de coordination efficaces et définir les processus de prise de décision et de communication ;
- Préparer et valider un plan détaillé pour la mise en place de l'architecture institutionnelle, identifier les étapes, les ressources nécessaires et les échéanciers, et définir des critères de suivi et d'évaluation. Le plan sera inclus dans le plan d'actions pour la mise en œuvre Stratégie Nationale sur la Cybersécurité et la Cybercriminalité au point 3.

3 Elaborer une Stratégie Nationale sur la Cybersécurité et la Cybercriminalité comprenant un plan d'actions pour sa mise en œuvre en employant la méthodologie du Guide pour le Développement d'une NCS ou autres bons pratiques reconnus. Pour cette tache le Consultant devra :

- Élaborer un plan de projet pour gérer le développement de la stratégie et du plan d'action. Celui-ci inclura toutes les tâches et étapes clés nécessaires à la réalisation réussie de la stratégie et du plan d'action, ainsi que les principales parties prenantes impliquées dans le processus ;
- Sur la base des rapports d'évaluation du risque et de capacité nationale en matière de cybersécurité au point 1, déterminer les priorités et les objectives stratégiques à inclure dans la Stratégie Nationale sur la Cybersécurité et la Cybercriminalité, et consulter les parties prenantes pertinentes pour valider les priorités et les objectifs stratégiques ;
- Rédiger la Stratégie Nationale sur la Cybersécurité et la Cybercriminalité en se basant sur les résultats du processus de consultation des parties prenantes et élaborer la version finale de la stratégie en vue de son approbation par le gouvernement ;
- En se basant sur les priorités et les objectifs stratégiques soulevées dans la Stratégie Nationale sur la Cybersécurité et la Cybercriminalité, élaborer un plan d'actions de mise en œuvre comprenant des initiatives chiffrées et hiérarchisées visant à concrétiser et opérationnaliser la stratégie. Consulter les parties prenantes pertinentes pour valider le document et élaborer la version finale du plan d'action en vue de son approbation par le gouvernement ;
- Rédiger les Termes de Référence, les spécifications techniques et la documentation d'appel d'offres préliminaire pour chacune des activités définies dans le plan d'actions de mise en œuvre.

4 Faciliter un atelier de formation (3 jours) pour présenter les livrables et supporter la formation du personnel clé. Pour cette tache le Consultant devra :

- Développer les modules de formation en se basant sur les principes et les meilleures pratiques de la cybersécurité, en mettant l'accent sur les aspects politiques et les procédures de la Stratégie Nationale sur la Cybersécurité et la Cybercriminalité au point 3, et sur modèle d'architecture institutionnelle pour la gestion de la cybersécurité au point 2 ;
- Adapter la formation aux besoins et objectifs du Burundi, et personnaliser la formation en conséquence ;
- Faciliter des séances de sensibilisation pour familiariser les participants avec les concepts clés de la cybersécurité et les sensibiliser aux risques et aux bonnes pratiques ;
- Dispenser une formation pratique sur l'élaboration de politiques de cybersécurité en leur fournissant des outils et des exemples concrets basés sur l'expérience du Burundi ;

- Faciliter des discussions et des échanges d'expériences et faciliter des discussions interactives pour favoriser l'apprentissage collaboratif.

La durée de la mission ne doit pas excéder cent quatre-vingts jours (180) calendaires.

Le consultant devra animer un atelier de lancement de la mission, ainsi que des ateliers de restitution des rapports d'étape et de validation de rapport final.

Le consultant doit proposer sa méthodologie détaillée pour l'atteinte des objectifs de la mission.

V. LIVRABLES ATTENDUS ET CALENDRIER DE RÉALISATION

Le consultant est tenu de mener à bien l'intégralité de la mission dans un délai de 26 semaines et de soumettre les livrables suivants, en se basant sur les échéanciers indicatifs et le calendrier de paiement détaillés ci-dessous. Les décaissements se feront sur la base des rapports jugés acceptables par le client tel que le précisera le contrat négocié.

. #	Echéance	Produits livrables	Décaissement
1.	Signature +1 semaine	Rapport de Cadrage/plan de la mission	10%
2.	Signature +7 semaines	Rapport d'évaluation de la capacité nationale en matière de cybersécurité (CMM) comme indiqué à l'activité 1	30%
3.	Signature +7 semaines	Rapport d'évaluation du risque en matière de cybersécurité comme indiqué à la tâche 1	
4.	Signature + 12 semaines	Modèle d'architecture institutionnelle pour la gestion de la cybersécurité qui définit les rôles et responsabilités au niveau national, et plan d'actions pour son implémentation comme indiqué à la tâche 2	40%
5.	Signature + 17 semaines	Stratégie Nationale sur la Cybersécurité et la Cybercriminalité comme indiqué à la tâche 3	
6.	Signature + 21 semaines	Plan d'actions de mise en œuvre de la Stratégie Nationale sur la Cybersécurité et la Cybercriminalité comme indiqué à la tâche 3	
7.	Signature + +24 semaines	Atelier de formation (3 jours) pour présenter les livrables et supporter la formation du personnel clé comme indiqué à la tâche 4	20%

. #	Echéance	Produits livrables	Décaissement
8.	Signature + 26 semaines	Rapport final de la mission	

VI. PROCÉDURE DE RAPPORT ET DE VALIDATION

Tous les livrables doivent être soumis au coordinateur de l'UGP, au spécialiste de l'UGP désigné et au point focal de MINCOTIM, dont les coordonnées seront communiquées ultérieurement. Les livrables écrits doivent être soumis électroniquement au format PDF et Word modifiable, permettant l'ajout de commentaires/modifications.

Un Comité technique de suivi ad hoc sera mis en place et chargé d'examiner chaque livrable et disposera d'une semaine pour fournir des commentaires et valider chaque livrable. Sur demande, le consultant pourra également être amené à présenter verbalement les livrables [en personne ou virtuellement] aux parties prenantes concernées, y compris MINCOTIM, UGP, etc., afin de recueillir des commentaires. Les livrables seront soumis pour revue technique et non objection par la Banque Mondiale. La validation des livrables sera faite par le Comité technique de suivi ad hoc.

VII. RESPONSABILITÉS DU CLIENT

Le MINCOTIM s'engage à fournir, dans la mesure de ses capacités, les éléments suivants :

- Toutes les données de référence et la documentation jugée pertinente pour mener à bien la mission et accomplir les tâches identifiées, à leur disposition immédiate.
- Un accès aux responsables clés des ministères/organismes/départements pertinents et d'autres entités officielles concernées, le cas échéant.
- Faciliter la coopération avec d'autres organisations dont les activités et programmes pourraient être considérés comme pertinents pour la mission.

VIII. EMPLACEMENT

Le bureau d'études doit être disponible pour travailler au Burundi, plus particulièrement avec le MINCOTIM et le PAFEN. Cependant, de commun accord avec le client, une partie de la mission pourra être effectuée à distance.

La collaboration avec des experts locaux, basés au Burundi pendant la durée de la mission est encouragée car cela facilitera la collecte des intrants nécessaires et la connaissance du contexte local.

IX. TRANSFERT DE CONNAISSANCES

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

X. CONSULTATION DES PARTIES PRENANTES

Le consultant devra travailler étroitement avec le spécialiste de l'UGP désigné, ainsi qu'avec un point focal du MINCOTIM qui sera le principal bénéficiaire de cette mission.

XI. PROFIL DU BUREAU ET QUALIFICATION DU BUREAU

Le consultant devra avoir les qualifications suivantes :

- Être un cabinet d'études/conseils doté de solides compétences et d'expériences en matière de cybersécurité et Technologies de l'Information et de la Communication, notamment dans les domaines suivants : gouvernance, législation, gestion des risques, protection des infrastructures d'information critiques, réponse aux incidents, développement des compétences en cybersécurité avec au moins 5 and une expérience pertinente
- Avoir réalisé au moins deux (2) missions similaires en Afrique subsaharienne de préférence dans un pays francophone
- Démontrer la compréhension des principaux cadres, méthodologies et meilleures pratiques en matière de cybersécurité, notamment : Guide pour le développement d'une stratégie nationale de cybersécurité, CMM, cadre de services CIRT, NISTCSF, ISO 2700x, etc.
- 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

Le Consultant mettra sur l'étude, un personnel clé qualifié ayant une grande expérience dans le domaine spécifique. Tout le personnel de l'équipe devra avoir une bonne connaissance du Français (écrit et parlé).

L'équipe alignée devra comprendre au moins les experts clés suivants, ainsi que tout autre personnel de soutien supplémentaire jugé nécessaire pour mener à bien la mission. Le consultant doit fournir un plan de personnel comprenant les noms, les rôles et les CV de l'équipe centrale dans le cadre de sa proposition.

Personnel clé	**Expérience**	**Qualifications**
(1) Chef d'équipe, ou équivalent	• Au moins 7 ans d'expérience dans l'industrie de la cybersécurité • Expérience dans la direction de projets de cybersécurité et connaissance des meilleures pratiques mondiales en matière d'élaboration de politiques de cybersécurité et de gouvernance. • Excellentes compétences en communication et en leadership, ainsi qu'une expérience dans la gestion de projets complexes. • Solides compétences en gestion de projet, avec la capacité d'élaborer des plans de projet, de gérer les ressources et de superviser les livrables du projet. • Expérience antérieure en réseautage et en collaboration avec des institutions gouvernementales.	Master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, science/technologie ou autres domaines pertinents.
(1) Spécialiste des politiques et de la gouvernance en matière de cybersécurité	• Au moins 5 ans d'expérience dans les politiques et la gouvernance en matière de cybersécurité, avec un accent sur les politiques, réglementations et normes de cybersécurité au niveau national. Expérience en matière de suivi et d'évaluation de la cybersécurité et de KPI pour le secteur public. • Capacité avérée à concevoir et mettre en œuvre des politiques et des réglementations en matière de cybersécurité, et à assurer la conformité aux normes et	Master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, science/technologie ou autres domaines pertinents.

Personnel clé	Expérience	Qualifications
	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.	
(1) Spécialiste de la gestion des risques et de la protection des infrastructures d'information critiques (CIIP)	• Au moins 5 ans d'expérience dans la gestion des risques et la CIIP, de préférence au niveau national. • Connaissance approfondie des cadres de gestion des risques et de la CIIP, tels que NIST SP 800-53, ISO/IEC 27001 ou CIP-014-1, et de leur application aux processus de protection des ICI. • Certifications pertinentes, telles que Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) ou Certified Critical Infrastructure Protection Professional (CCIPP), très souhaitées.	Master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, science/technologie ou autres domaines pertinents.

Cette équipe devra être complétée par une expertise locale d'appui hautement qualifiée et qui devrait se voir attribuer un rôle et une part substantielle du travail.

XII. FINANCEMENT DE LA MISSION

La mission d'assistance technique sera financée par le Projet d'Appui aux Fondations de l'Economie Numérique (PAFEN). Le coût de l'atelier de validation de l'étude sera pris en charge directement par le Projet.

XIII. METHODE DE SELECTION DU BUREAU

Le bureau de consultants sera sélectionné selon la méthode de Sélection fondée sur la qualité et le coût (SFQC) conformément au Règlement de Passation des Marchés pour les Emprunteurs

sollicitant le financement de Projets d'Investissement (FPI), édition de juillet 2016, révisé en novembre 2017, août 2018 et novembre 2020 et conformément aux critères exigés au regard des présents termes de référence.