TERMES DE REFERENCES

RECRUTEMENT D'UNE FIRME POUR ASSURER L'ASSISTANCE TECHNIQUE EN CYBERSÉCURITÉ ET PROTECTION DES DONNÉES

A. Contexte

1. Le Gouvernement de Madagascar a obtenu un financement de l'Association internationale de développement (IDA ou Banque mondiale) pour appuyer les réformes dans le cadre du Projet de gouvernance digitale et de gestion de l'identité malagasy (Crédit 6780-MG (« **Projet** »).

2. La Composante 1 du Projet vise à combler les lacunes et à réduire les inefficacités du système de gestion de l'identité actuel. Les objectifs consistent à : (i) faciliter et sécuriser l'accès de tous les citoyens aux services d'enregistrement des faits d'état civil et à l'identité juridique ; et (ii) fournir les fondements institutionnels et technologiques en appui à la simplification de l'accès aux services et prestations publics ainsi que les efforts de transformation digitale. Cela comprend la création de bases de données nationales d'enregistrement des faits d'état civil et d'identité ; l'adoption et la mise en œuvre d'un numéro d'identification unique dès la naissance et l'amélioration de la sécurité des pièces d'identité ; le renforcement du cadre réglementaire et juridique pour sécuriser les données et protéger les données à caractère personnel ; la mise en place des bases d'une vérification et d'une authentification d'identité numérique améliorées permettant aux citoyens d'accéder aux services et aux prestations ; la numérisation des processus et des registres d'enregistrement des faits d'état civil en vue de la mise en œuvre d'une base de données nationale sécurisée consolidée de l'identité ; et la mise en œuvre des registres fondamentaux (identité et enregistrement des faits d'état civil), sur lesquels les plateformes numériques publiques reposeront et qui seront mis en relation à travers le système d'interopérabilité.

3. Le Gouvernement a adopté la Stratégie nationale de réforme de l'enregistrement des faits d'état civil en 2017 et une nouvelle législation en 2018 (loi n° 2018-027 régissant les registres de l'état civil), qui plaide pour la création d'un Centre National d'Etat Civil et d'Identification (« CNECI ») pour gérer le registre de l'état civil central et les bases de données nationales d'identification, qui constitueront la base de la délivrance des pièces d'identité. Un décret a été adopté le 2 décembre 2020 pour institutionnaliser la création du CNECI, qui sera opérationnalisé avec l'appui de PRODIGY.

4. La Composante 2 du Projet vise à appuyer la rationalisation et la numérisation des services publics et à accroître la fourniture, la couverture et la qualité des services publics, en renforçant les infrastructures et la capacité de l'administration à fournir des services publics plus rapides, moins chers et de meilleures qualités. Les objectifs consistent à : (i) renforcer la capacité du gouvernement à rationaliser et fournir des services publics à travers de multiples canaux (exemple : en ligne, vocal, hors ligne tel que SMS ou USSD) ; et (ii) à fournir des infrastructures institutionnelles et technologiques (dorsales et frontales) qui appuient la fourniture des services.

5. Le Projet est géré par une Unité de Coordination de projet (« **UCP** »), relevant de la Présidence. L'UCP collabore étroitement avec l'Unité de Gouvernance Digitale (« UGD »), qui est chargée d'élaborer et de mettre en œuvre la Stratégie de transformation digitale du gouvernement, et le Coordination Générale du PREA, qui est chargé d'appuyer les réformes de l'administration publique.

6. La Présidence a créé l'UGD, avec l'aide de PRODIGY, pour élaborer la stratégie nationale de gouvernance digitale et coordonner sa mise en œuvre. La stratégie repose sur les pratiques d'excellence internationales incluant une approche de conception agile et centrée sur l'utilisateur. Un Chief Digitale Officer (« CDO») a été recruté en décembre 2019 pour diriger l'UGD. Le Gouvernement met actuellement en place le reste de l'équipe au sein de l'UGD, et le CDO a commencé à revoir et à appuyer le développement des différents services numériques basés sur les pratiques d'excellence internationales.

7. Le manque de sécurisation des données et de respect de la vie privée ne favorise pas la confiance dans les services digitaux publics et privés et crée des risques pour tous les utilisateurs. Madagascar a adopté une loi sur la protection des données en 2014 (loi n° 2014-038) et une législation plus récente relative à la cybersécurité et la cybercriminalité a été adoptée en 2016 (loi n° 2016-031 amendant la loi n° 2014-006). Toutefois, les cadres réglementaires, opérationnels et institutionnels faisant toujours défaut, l'Equipe d'intervention en cas d'urgence informatique (« CIRT ») ainsi que l'autorité de protection des données connue sous le nom de Commission Malagasy de l'Informatique et des Libertés (« CMIL ») n'ont pu être établis. Le CIRT devrait être créé au sein de l'Autorité de Régulation des Télécommunications (ARTEC), tandis que la CMIL sera créée au sein du Ministère de la Justice, en étroite collaboration avec l'UGD. Aucune politique gouvernementale n'existe sur la propriété et l'utilisation des données, ni aucune autorité de surveillance opérationnelle garantissant la confidentialité des données. Les mesures techniques et organisationnelles de sécurisation des données à caractère personnel de la loi n° 2018-027 régissant les registres de l'état civil ne sont pas pleinement mises en œuvre. Le manque de formation des fonctionnaires accentue également les risques de balayage massif de données. En conséquence, les systèmes digitaux publics de Madagascar figurent parmi les plus vulnérables au monde[1]. Une Revue de la capacité en cybersécurité a été réalisée en 2016 par le Centre mondial des capacités de cybersécurité (GCSCC), relevant des lacunes et des défis importants.

8. La CMIL est l'autorité en charge du suivi et du contrôle du traitement des données à caractère personnel. Il s'agit d'une autorité administrative indépendante créée par la loi n° 2014-038 sur la protection des données. Toutefois, des réformes réglementaires sont encore nécessaires pour son organisation et son opérationnalisation. L'élaboration du décret d'application nécessite une étude approfondie de systèmes similaires dans d'autres pays ainsi que la formulation de recommandations claires et précises pour orienter la politique générale de l'Etat.

9. Des réformes juridiques, réglementaires et institutionnelles sont nécessaires pour garantir que le Projet est mis en œuvre conformément aux exigences en matière de cybersécurité et de protection des données. En prévision de ces mises au point, le Gouvernement cherche à recruter des consultants dans le cadre du Projet pour dispenser des conseils, entre autres, sur les besoins de renforcement des capacités institutionnelles, juridiques et réglementaires, tel qu'indiqués dans les présents TdR.

B. Objectifs

10. Le Gouvernement de Madagascar souhaite recruter les services d'un cabinet de conseil ou d'un consortium de cabinets (« Consultant ») qui fournira une assistance juridique, opérationnelle et technique à l'UGD, au Ministère de la Justice et à l'ARTEC, dans la mise en œuvre du cadre

[1] Madagascar figure au 98ème rang sur 100 pays à l'Indice de cybersécurité 2018 (NCSI 2018)

juridique existant et dans le renforcement des capacités institutionnelles et réglementaires pour permettre une mise en application effective des réformes envisagées par le projet. L'objectif primordial est d'instaurer un environnement de certitude et de confiance dans la transformation digitale à Madagascar.

11. Le Consultant affectera un « Conseiller résident » pour une assistance au quotidien et celui-ci collaborera étroitement avec l'UGD, le Ministère de la Justice, l'ARTEC, le CIRT, la CMIL et les institutions appuyées par le Projet dans le domaine de la transformation digitale - le cas échéant, afin d'assurer une bonne exécution du Projet, en particulier, en ce qui concerne la protection des données à caractère personnel, la cybersécurité et les transactions numériques.

C. Teneur de la mission

12. La mission porte sur trois principaux domaines : (i) renforcer les capacités institutionnelles et humaines (des parties prenantes indiquées au point n° 10) ; (ii) combler les lacunes du cadre juridique ; (iii) combler les lacunes techniques en matière de cybersécurité et de protection des données ; et (iv) fournir les services d'un Conseiller résident.

13. Dans l'exécution de sa mission, le Consultant adoptera une approche qui favorise la confiance, la transparence et la redevabilité, des caractéristiques qui devront se retrouver dans le cadre juridique, réglementaire et institutionnel mais aussi dans les services de conseil rendus. En particulier, le montage institutionnel visera à promouvoir l'ouverture dans la mesure du possible, promouvant des discussions régulières avec le secteur privé et la société civile ainsi que des rapports et une communication fréquente, y compris sur les échecs éventuels.

14. Avant la mission, le Consultant examinera la situation à Madagascar et en acquerra une bonne compréhension, y compris ce qui concerne les institutions participantes, les lois, les réglementations et les politiques existantes actuellement applicables (énumérées ci-après), mais aussi les rapports et les travaux des consultants actuels et précédents qui seront mis à sa disposition.

- Loi n° 2014-038 sur la protection des données ;
- Loi n° 2016-031 sur la cybersécurité et la cybercriminalité ;
- Loi n° 2018-027 régissant les registres de l'état civil ;
- Loi n° 2014-024 sur les transactions électroniques ;
- Loi n° 2014-025 sur la signature électronique ;
- Document d'évaluation de projet préparé par la Banque mondiale ;
- Rapport d'analyse juridique communiqué en décembre 2019 par Cameron McKenna Nabarro Olswang LLP.

15. Le Consultant mènera une évaluation des écarts et une évaluation rapide des lacunes existantes en matière de capacité et de compétence institutionnelles à travers des entretiens avec les principales parties prenantes ainsi qu'un examen de la documentation existante et des rapports préparés par les consultants recrutés par l'UCP pour mener les réformes juridiques et fournir une assistance technique.

(i) Renforcement des capacités institutionnelles et humaines

16. Le Consultant appuiera la mise en place opérationnelle du CIRT et de la CMIL (les institutions) à travers les tâches suivantes :
   a. Rédiger le règlement d'application visant à opérationnaliser les institutions ;
   b. Affiner le budget nécessaire pour mettre en œuvre les stratégies pertinentes ;
   c. Etablir un organigramme détaillé des institutions nouvellement créées ;

d. Rédiger tous les termes de référence techniques du personnel des institutions, établir la composition des différents comités et définir les tâches à réaliser par tous les autres acteurs concernés par les questions d'identification, de cybersécurité et de protection des données ;
e. Préparer les critères de sélection et de nomination des instances dirigeantes de la CNECI et du CIRT, et contribuer aux critères de sélection et de nomination aux postes de la CMIL énumérés à l'Article 29.1 de la Loi 2014-038 à inclure dans un projet de décret, conformément à l'Article 29.2
f. Aider dans le recrutement et la formation du personnel, y compris définir les critères d'évaluation et les questionnaires pour l'entretien, aider dans l'évaluation de la qualification des candidats et dans la sélection des candidats finaux ;
g. Rédiger les manuels opérationnels des institutions et toute autre documentation pertinente pour assurer une bonne gouvernance de ces institutions (tels que les codes de conduite) ;
h. Rédiger les Codes de conduite de tout le personnel, de la direction et des membres du Conseil ;
i. Opérationnaliser les institutions, y compris aider la direction et les membres du Conseil dans l'établissement d'un programme de travail comprenant les objectifs et les indicateurs détaillés à réaliser, et organiser des ateliers avec les parties prenantes concernées pour présenter les activités à mettre en œuvre et en convenir ;
j. Renforcer la capacité du personnel nouvellement recruté à réaliser les objectifs fixés par les institutions dans le cadre du Projet et les autres parties prenantes ;
k. Appuyer l'élaboration et la mise en œuvre d'une stratégie de communication et de sensibilisation dans le but d'instaurer la confiance dans les institutions nouvellement créées et la digitalisation en général ;
l. Contribuer à la conception et à la mise en œuvre d'un programme national de formation sur la cybersécurité et la protection des données, à mettre en œuvre par l'UGD à travers le centre de formation. Le programme comprendra une formation spécialisée mais aussi une formation de base pour tous les fonctionnaires. Les conseils dispensés comprendront des recommandations sur l'élaboration du modèle opérationnel approprié, tel qu'un appui apporté par des établissements de formation internationaux pour la mise en place de nouveaux programmes d'enseignement dans les établissements universitaires publics ou privés locaux ; et
m. Prendre en charge tout autre aspect qui serait raisonnablement pertinent pour la mise en œuvre des activités décrites ci-dessus et qui pourrait être convenu entre le Consultant et le Gouvernement de Madagascar au cours de cette mission de conseil.

(ii) Combler les lacunes du cadre juridique

17. Le Consultant élaborera un plan pour combler les lacunes du cadre juridique et rédigera les instruments nécessaires pour favoriser un environnement de certitude et de confiance favorable à l'adoption et à la promotion de l'économie digitale, y compris pour favoriser les transactions et les interactions de gouvernement-à-gouvernement, de citoyen-à-gouvernement et d'entreprise-à-gouvernement. Le plan sera basé sur une étude préalable et l'analyse approfondie du cadre juridique et réglementaire de Madagascar, un aperçu comparatif des pratiques d'excellence internationales et des recommandations sur les réformes à adopter pour mettre en vigueur les réformes envisagées dans ce Projet. Il comprendra les aspects énumérés au point C.15, ainsi que les suivants. L'assistance juridique spéciale portera sur les aspects substantifs de la loi suivants :
    a) Enregistrement des faits d'état civil et identité
        - En étroite coordination avec les institutions et agences concernées, rédiger le décret d'application de la loi sur l'enregistrement des faits d'état civil (loi n° 2018-027) ;
        - Rédiger tout autre texte juridique ou réglementaire nécessaire à la mise en œuvre des réformes, en se basant sur une analyse préexistante du cadre juridique et réglementaire, l'assistance technique continue fournie pour l'opérationnalisation des réformes (en particulier, pour la mise en place de la CNECI), les consultations avec les parties prenantes, et toute analyse complémentaire de la réforme juridique et réglementaire.
    b) Protection des données et cybersécurité

- Mener une analyse approfondie du cadre juridique et réglementaire malagasy en rapport à la protection des données et la cybersécurité ;
- Formuler des recommandations visant à améliorer le cadre juridique et réglementaire, et à orienter un cadre gouvernemental de protection des données et de cybersécurité qui soit fondé sur les pratiques d'excellence internationales. A ce titre, une présentation et une étude comparative seront effectuées sur les systèmes appliqués dans d'autres pays pour contrôler et traiter les données à caractère personnel.
- Rédiger le décret d'application de la loi n° 2014-038. Ce décret comprendra les détails de l'organisation et de l'opérationnalisation de la CMIL, une description détaillée des attributions de la CMIL mentionnées à l'Article 37 de la Loi n° 2014-038, et l'organigramme de la CMIL.

(iii) Combler les lacunes techniques en matière de cybersécurité et de protection des données

18. Le Consultant fournira un appui direct afin d'assurer que les normes internationales de cybersécurité et de protection des données soient mises en pratique en ce qui concerne les logiciels, les bases de données et l'infrastructure informatique, et formera l'équipe de sécurité au sein de l'UGD, du CIRT et des institutions appuyées par le projet. Cet objectif sera réalisé à travers une assistance technique pour un audit de sécurité, notamment des analyses d'évaluation de la vulnérabilité et des tests d'intrusion.

Analyse de la vulnérabilité et renforcement de capacité

19. Les analyses de la vulnérabilité devraient aider l'UGD et les institutions bénéficiaires du Projet à combler de manière proactive toute lacune et à maintenir un environnement de sécurité solide pour les systèmes publics, les données, les citoyens et les fonctionnaires. Les analyses devraient indiquer :
    - Les correctifs manquants et les vulnérabilités connues ;
    - Les faiblesses dans le paramétrage de la sécurité telles que les mots de passe par défaut ou l'insuffisance de cryptage ;
    - Les paramètres de services réseau non sécurisés ;
    - Les problèmes courants des application web ou les atteintes à la sécurité des données ;
    - Les paramètres technologiques pouvant nécessiter des tests d'intrusion.

20. Le Consultant renforcera également la capacité de 30 fonctionnaires sur l'utilisation de SonarQube à produire des rapports sur la couverture des tests de codage (nombre de lignes de code couvertes par les tests), sur la qualité du codage (détection stylistique générale) et sur les tests de sécurité (exemple : analyse complète de toutes les vulnérabilités OWASP).

Tests d'intrusion

21. Le Consultant devra :
    - Concevoir des tests de sécurité appropriés pour les applications sélectionnées afin d'évaluer la sécurité des serveurs, des applications et des bases de données ; et effectuer ces tests. Tous les tests devront être approuvés par l'ARTEC et l'UGD, et les résultats seront présentés dans le rapport d'évaluation de la sécurité.
    - Effectuer des tests d'intrusion des serveurs et des applications.
    - Vérifier la conformité du codage des applications aux normes de qualité de codage.
    - Rechercher les failles de sécurité dans le codage des applications, y compris le codage côté client, le codage côté serveur et les communications entre les clients et le serveur.
    - Les tests devraient porter sur les failles de sécurité courantes telles que la redirection et le transfert non autorisés, les attaques par injection de commandes SQL, les attaques par

injection de RCFL, les attaques de type CRSF, les attaques par injection SSI et les scripts intersites (XSS).

- Examiner l'environnement des applications sur les serveurs, y compris les paramètres de sécurité des systèmes d'exploitation et des serveurs web ; examiner la sécurité d'accès aux fichiers et répertoires. Veiller à ce que toutes les mises à jour nécessaires soient effectuées dans les services de support et identifier les composantes présentant des vulnérabilités connues.
- Tester la gestion de l'accès, y compris examiner la sécurité des mots de passe et des informations d'identification des utilisateurs, ce qui comprend le traitement de l'entrée et de la sortie des données des utilisateurs et l'exposition aux données à caractère sensible.
- Evaluer la sécurité des bases de données à partir du codage de l'application et sur le serveur, y compris tester les accès non autorisés, l'exposition aux données à caractère sensible, le nettoyage correct des données et les risques d'injection de code SQL.
- Evaluer les procédures de reprise après sinistre et formuler des recommandations sur les améliorations à apporter.
- Examiner la disponibilité, la fiabilité et la performance des applications en tenant compte de leur base d'utilisateurs et des prévisions de croissance de la base d'utilisateurs.
- Pour chaque test d'intrusion, le Consultant devra produire un rapport d'évaluation de sécurité présentant ses conclusions et des recommandations, qui comprennent : i) une liste des tests effectués, avec les résultats de chaque test dans une feuille de calcul associée ; ii) un tableau qui énumère et décrit chaque vulnérabilité, la solution pour y remédier, la catégorie, la conformité, les vulnérabilités et les expositions courantes, les adresses IP affectées et le niveau de risque ; iii) un récapitulatif qui détaille l'accès au site et la gestion de ces accès ; iv) une revue de l'environnement des applications sur le serveur, y compris les paramètres de sécurité du système d'exploitation et du serveur web ; une revue de la sécurité d'accès aux fichiers et aux répertoires ; v) une évaluation des procédures de reprise après sinistre ; vi) une liste de recommandations sommaires séparément dans une annexe au rapport ; et vi) toute autre information ayant trait aux résultats des tests.

22. L'ARTEC et l'UGD mettront à disposition les informations et/ou accorderont l'accès avant l'audit. Le Consultant recevra une Identité d'utilisateur standard. Les tests **doivent** chercher à identifier les vulnérabilités d'un point de vue à la fois externe (pour le Frontal numérique [DFE]) mais aussi interne. Tous les tests d'intrusion **doivent** être conçus pour réduire au minimum le risque d'accès aux données à caractère personnel par les testeurs d'intrusion. Les tests **doivent** combiner les techniques automatisées et les techniques manuelles et respecter la norme d'exécution des tests d'intrusion (PTES). Les vulnérabilités devraient être constatées mais non exploitées, c'est-à-dire que l'exécution des tests ne devraient pas être destructive. Les propositions **doivent** expliquer la méthodologie adoptée pour répondre à cette exigence. Lorsque les noms de fichier ou de table de base de données ne semblent pas indiquer un contenu composé de données à caractère personnel, ceux qui contiennent des données sensibles à caractère personnel, une fois ouvert, **doivent** immédiatement être fermés.

(iv) Conseiller résident

23. Le Consultant affectera un Conseiller résident qui travaillera au sein de l'UGD, de l'ARTEC et du Ministère de la Justice en tant que point focal principal pour tous les aspects en rapport à la protection des données. Le rôle du Conseiller résident consistera à :
    - Etablir les processus et les procédures internes et externes ;
    - Etablir les prises de décision et les considérations administratives nécessaires ;
    - Mettre en place des processus et des procédures de traitement des commentaires et des questions des personnes concernées concernant le traitement de leurs données à caractère personnel par les trois entités énumérées précédemment ;

- Former le personnel des trois entités indiquées précédemment et renforcer leur capacité sur leurs obligations en vertu de la loi n° 2014-038 sur la protection des données à caractère personnel et de toute réglementation applicable, et le personnel des institutions appuyées par le projet, le cas échéant ;
- Faire le suivi de la conformité des trois entités visées à la loi n° 2014-038 sur la protection des données à caractère personnel et à tout autre texte applicable, ainsi que former le personnel sur la mise en conformité et réaliser des audits ;
- Etablir des processus et des mécanismes appropriés pour la conformité en matière de protection des données ;
- Coopérer avec l'autorité de surveillance de la protection des données, la CMIL, une fois qu'elle est établie ; et
- Agir en tant que ressource et point focal pour les questions de protection des données qui ont trait à ce qui précède dans les limites du raisonnable.

D. Produits livrables et calendrier

24. Les services de conseil seront à fournir sur une période 24 mois. Les produits livrables et les délais indicatifs sont comme suit :

	Produits livrables	**Date d'échéance du produit livrable (signature du contrat + x semaines)**
1.	Rapport de démarrage comprenant la priorisation des travaux : évaluation des écarts, calendrier détaillé des activités à mettre en œuvre à travers l'assistance technique, y compris le plan de travail en version provisoire pour le Conseiller résident	4 semaines
	Renforcement de capacité	
2.	Rapport initial sur les questions traitées au point C.15	8 semaines
3.	Rapport intermédiaire sur les questions traitées au point C.15	32 semaines
4.	Rapport final sur les questions traitées au point C.15	52 semaines
	Cadre juridique	
5.	Rapport initial sur les questions traitées au point C.16	8 semaines
6.	Rapport intermédiaire sur les questions traitées au point C.16	32 semaines
7.	Rapport final sur les questions traitées au point C.16	52 semaines
8.	Ajouter un calendrier pour le renforcement de capacité technique en Cyber & Données	
	Conseiller résident	
9.	Mobilisation du Conseiller	8 semaines
10.	Plan de travail final du Conseiller résident	8 semaines
11.	Rapports du Conseiller résident	Chaque mois[2]

[2] Pendant 12 mois après mobilisation

E. Dispositif administratif

Le Consultant rendra compte à l'ARTEC pour la cybersécurité et au Ministère de la Justice pour la protection des données, et assurera également la communication avec le Gouvernement et les parties prenantes externes, et les consultera, si nécessaire. Les parties prenantes comprennent l'UGD, le PREA, les ministères de tutelle du GOUVERNEMENT (tels que le Ministère de l'Intérieur et de la Décentralisation ; le Ministère de l'Economie et des Finances ; le Ministère du développement Numérique, de la transformation Digitale, des Postes et des Télécommunications), les partenaires au développement (Banque mondiale), les entités du secteur privé, les organisations de la société civile et les fournisseurs de technologies. Le Consultant considérera et traitera comme confidentiels tous les documents et toutes les communications dans le cadre de cette mission.

Le Consultant devrait préparer une documentation succincte et pertinente pour étayer toutes les recommandations et discuter des recommandations avec les parties prenantes dans le pays. Sauf disposition contraire dans ces TdR, tous les produits livrables et rapports seront rédigés en français et présentés au format Word, Excel et Powerpoint, ou équivalent. Les versions préliminaires des produits livrables seront soumises par voie électronique, et les versions successives des rapports comprendront des marques de suivi des changements par rapport à la version précédente. Des exemplaires de tous les produits livrables seront fournis à l'UGD et à la Banque mondiale.

F. Qualifications du Consultant et du Conseiller résident

- Le Consultant doit être un cabinet ou un consortium de cabinets ayant démontré trois (3) expériences réussies dans la fourniture d'assistance technique aux gouvernements, dans les domaines suivants : identification numérique, protection des données, cybersécurité, transaction numérique au cours des cinq (5) dernières années ;
- Le Consultant doit disposer d'au moins deux (2) expériences réussies dans la conduite de travaux similaires au cours des cinq (5) dernières années ;
- Le Consultant aura au moins deux (2) ans d'expérience dans la mise en place d'institutions de réglementation ainsi que des connaissances et de l'expérience confirmées dans les domaines de travail décrits dans ces TdR (en particulier, la protection des données et la cybersécurité) ;
- L'équipe du Consultant doit comprendre des spécialistes juridiques, règlementaires et technique ayant chacun minimum douze (12) ans d'expériences dans leurs domaines d'expertises respectifs ;
- Tout le personnel du Consultant travaillant avec le Gouvernement parlera couramment le français ou sera assisté par des interprètes.
- Une expérience des pays en développement sera un atout.

.