REPUBLIQUE DEMOCRATIQUE DU CONGO

PROJET DE TRANSFORMATION NUMÉRIQUE

PROJET N° P180495

ZR-UGP - PTN-537385-CS-QCBS

TERMES DE RÉFÉRENCE POUR ÉLABORATION DE LA STRATÉGIE INTEGRÉE DE L'IDENTIFICATION ET DU SCHÉMA DIRECTEUR DU SYSTÈME NATIONAL D'IDENTIFICATION DE LA POPULATION (SNIP) EN RDC

Mars 2026

TABLES DES MATIERES

1. INTRODUCTION

Le Gouvernement de la République Démocratique du Congo (RDC) a reçu un appui de l'Association Internationale pour le Développement (IDA) du Groupe de Banque Mondiale et Agence Française de Développement (AFD) pour réaliser le Projet de Transformation Numérique (PTN) de la RDC (« le Project »), qui sera mis en œuvre entre 2025 et 2029.

L'objectif de développement du Projet est d'accroître l'accès et l'utilisation de l'internet et renforcer les bases des services numériques en RDC. Pour ce faire, le Projet investira dans (i) l'infrastructure de connectivité numérique fondamentale nécessaire pour soutenir le mouvement vers l'accès numérique universel ; (ii) l'infrastructure publique numérique (DPI) requise pour permettre aux secteurs publics et privés de développer des services numériques intégrés, ouverts et sécurisés au niveau sectoriel ; (iii) le renforcement de la base de compétences numériques avancée et l'écosystème d'innovation numérique de la RDC pour garantir l'utilisation productive de la technologie, favorisant la création d'emplois et soutenant le développement de nouveaux services numériques, et (iv) le renforcement de la capacité institutionnelle et la gouvernance nécessaires pour mener ces initiatives de manière concertée et intégrée.

Le Projet est constitué de 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 infrastructures et plateformes numériques partagées nécessaires pour étendre la fourniture de services numériques à travers la RDC, tout en soutenant leur intégration dans les secteurs clés pour améliorer l'accès aux services. Elle se concentrera sur les éléments fondamentaux de l'infrastructure DPI qui permettrait au gouvernement de favoriser l'innovation et d'étendre son utilisation des outils numériques.

- Composante 3 - Développer une main-d'œuvre compétente et stimuler l'innovation dans les services numériques : Cette composante visera à mettre en œuvre des programmes de formation pour renforcer 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 pour 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 environnementaux et sociaux (E&S).

La mise en œuvre est dirigée par le ministère des Postes et Télécommunications (MPT), où une Unité de Gestion du Projet a été créée, en collaboration avec d'autres parties prenantes, telles que le ministère de l'Économie numérique, l'Autorité de Régulation de la Poste et des Télécommunications (ARPTC), le Fonds de développement des services universels (FDSU), ministère de l'Intérieur, ministère de l'Enseignement supérieur et universitaire, ministère de l'Industrie et des PME, etc.

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 dans d'autres provinces de la République.

Ce projet s'inscrit dans le cadre d'un programme régional plus large implémenté à travers plusieurs pays d'Afrique orientale et australe, financé par la Banque mondiale, qui comprend un appui au COMESA (Marché commun de l'Afrique orientale et australe) afin de renforcer la coordination régionale et l'intégration économique. Cette collaboration régionale sera reflétée dans certaines des tâches décrites ultérieurement.

Pour plus de détails sur le projet, veuillez consulter le document du projet : https://documents1.worldbank.org/curated/en/099061024103010133/pdf/BOSIB130fc11f60601aa191c219a13fc1e5.pdf - veuillez vous référer à l'annexe 3 pour une description du projet en RDC.

Dans le cadre de la Composante 2 du Projet, une assistance technique est prévue pour appuyer le gouvernement dans la préparation et la planification de son programme national d'identité numérique. Celle-ci devra aboutir au développement d'un schéma directeur comprenant la stratégie de mise en œuvre, les spécifications techniques et fonctionnelles, et les modèles de gouvernance pour le futur système d'identification.

2. CONTEXTE ET JUSTIFICATION

La République Démocratique du Congo (RDC) s'est engagée, à travers le **Plan National du Numérique (PNN) Horizon 2025** et le **Plan d'action du Gouvernement 2025-2028**, à doter chaque citoyen d'une identité fiable, unique et interopérable. Cette

ambition s'inscrit dans la réalisation de l'**ODD 16.9** (« doter tous les individus d'une identité juridique d'ici 2030 »), mais également dans la volonté d'établir les bases d'une **infrastructure numérique publique robuste,** favorisant la prestation sécurisée des services publics et privés.

À ce jour, l'écosystème d'identification en RDC demeure fragmenté : de nombreux systèmes fonctionnels (ONIP, INSS, DGI, CENI, Ministère de la Santé, Police, etc.) coexistent, chacun jouant de facto le rôle d'identifiant, sans interconnexion avec un registre unique de la population. Cette multiplicité entraîne des doublons, des incohérences, des coûts élevés et une faible fiabilité des données. Les registres d'état civil, majoritairement manuels, souffrent également d'importantes pertes d'informations et ne sont pas intégrés à un fichier central.

Dans ce contexte, l'existence de différents systèmes fonctionnels n'est pas en soi un problème ; le véritable défi réside dans leur **absence de rattachement à un Registre National unique**, condition nécessaire pour garantir l'unicité de l'identification des personnes et la fiabilité des données utilisées par l'État et ses partenaires.

Avancées gouvernementales et mutualisation

Conformément à la vision consensuelle du Gouvernement, des efforts ont été déployés pour amorcer la **mutualisation des données d'identification** au travers du **Fichier Général de la Population (FGP)**. Sous l'impulsion de la Primature et avec l'appui de l'ONIP et du Ministère de l'Intérieur, plusieurs initiatives ont été lancées sur les plans juridique, institutionnel et technique afin de poser les bases de ce registre central. Ces efforts reflètent une volonté claire de rationaliser les investissements, de réduire les doublons et de disposer d'une base de données nationale fiable.

Toutefois, ces démarches de mutualisation nécessitent aujourd'hui une **vérification et une consultation élargie des parties prenantes** pour confirmer l'orientation à suivre, préciser le rôle de chaque institution et consolider un cadre de gouvernance consensuel. La stratégie intégrée et le schéma directeur devront ainsi évaluer les progrès réalisés, capitaliser sur les acquis et proposer les ajustements nécessaires pour une mise en œuvre durable et inclusive.

Nécessité d'un audit technique et organisationnel de l'ONIP

Dans ce processus, l'Office National d'Identification de la Population (ONIP), en tant qu'institution clé du dispositif national d'identification, joue un rôle stratégique dans la mise en œuvre opérationnelle du Système National d'Identification de la Population (SNIP) et dans la gestion des composantes liées à l'identification biométrique et à la production des titres d'identité.

Cependant, afin de garantir l'alignement entre les ambitions stratégiques nationales et les capacités réelles de mise en œuvre, il est indispensable de réaliser un audit technique et organisationnel approfondi de l'ONIP. Cet audit permettra notamment :

- D'évaluer l'architecture technique existante (infrastructures, systèmes d'information, biométrie, sécurité, interopérabilité, continuité des services) ;
- D'analyser la gouvernance institutionnelle, les processus opérationnels et les mécanismes de coordination interinstitutionnelle ;
- D'évaluer les capacités humaines, organisationnelles et financières de l'ONIP ;
- D'identifier les écarts entre la situation actuelle et les exigences d'un SNIP conforme aux standards internationaux ;
- De proposer une feuille de route de renforcement institutionnel, technique et organisationnel de l'ONIP, alignée avec la stratégie nationale d'identification.

Les résultats de cet audit devront alimenter directement l'élaboration de la stratégie intégrée d'identification et du schéma directeur du SNIP, afin d'assurer la faisabilité technique, institutionnelle et opérationnelle des orientations stratégiques proposées.

Nécessité d'une stratégie intégrée

La mise en place d'un **Système National d'Identification de la Population (SNIP)** constitue le socle de l'infrastructure numérique publique de la RDC. Le SNIP permettra :

- L'identification biométrique et biographique univoque de la population ;
- La constitution et la gestion du **Fichier Général de la Population (FGP)** ;
- La production et la distribution de la **Carte d'Identité Nationale** ;
- Le développement d'un service d'authentification et d'une **identité numérique souveraine** utilisable dans les transactions électroniques ;
- L'interopérabilité avec les registres sectoriels (état civil, fiscalité, protection sociale, éducation, santé, élections, etc.).

Une stratégie nationale intégrée est donc indispensable pour éviter la duplication des systèmes, garantir l'interopérabilité et assurer l'inclusion socio-économique. Elle permettra également de renforcer la protection des données personnelles, de promouvoir la cybersécurité et de mobiliser les partenaires techniques et financiers autour d'une vision claire, cohérente et soutenable.

L'importance d'une **vision maîtresse unique** : un **Schéma Directeur du Système National d'Identification de la Population (SNIP)** intégrant le cycle complet « enregistrement – gestion – utilisation – protection » de l'identité.

Le Gouvernement de la RDC s'est donc engagé à mettre en place un Système National d'Identification de la Population (SNIP) qui constituera le socle de l'infrastructure numérique publique nationale. Le SNIP permettra d'identifier les citoyens de manière univoque et fiable, en produisant par la suite une identité numérique souveraine, déclinée du numéro d'identification national (NIN) et qui sera utilisée lors des transactions électroniques sur des plateformes digitales certifiées.

La mise en place d'un Système National d'Identification de la Population (SNIP) doit comprendre les composantes ci-après :

1. L'identification de la population ;
2. La constitution et la gestion du Fichier Général de la Population ;
3. La production, gestion et distribution de la Carte d'Identité Nationale ;
4. La modernisation et l'optimisation de l'opérationnalisation du Bureau central des actes de l'état civil en tant que service central qui tient et entretient le fichier de l'état civil ;
5. Le système d'authentification sécurisé des identités et l'interface avec les fichiers fonctionnels du pays (état civil, assurances, banques, scolarité, transferts sociaux...) ;
6. La création de l'identité numérique pour l'accès aux services numériques gouvernementaux en ligne et d'autres prestations numériques ;
7. Le renforcement des capacités des acteurs publics et privés impliqués dans l'écosystème de l'identification en RDC.

Ces composantes soutiendront également l'intégration des services à fort impact tels que l'identifiant unique (identité numérique), la signature électronique, les paiements digitaux, les demandes de services administratifs en ligne (état civil, passeport, permis de conduire, permis de construire, etc.).

Objet de la mission

Le Gouvernement de la RDC souhaite recruter un cabinet pour mener une étude qui devra aboutir :

- À la réalisation d'un audit technique et organisationnel de l'ONIP ;
- À l'élaboration d'une stratégie nationale intégrée de l'identification ;
- À l'élaboration d'un schéma directeur du SNIP couvrant l'ensemble des composantes du système ;
- À la définition de feuilles de route opérationnelles pour l'identification biométrique de la population (Projet n° 3 du PNN) et la création de l'identité numérique (Projet n° 49 du PNN).

Le cabinet devra analyser l'écosystème national de l'identité actuel, intégrer les résultats de l'audit de l'ONIP et définir un schéma directeur conforme aux standards

Official Use Only

internationaux, ainsi que préparer des plans d'opérationnalisation réalistes, soutenables et alignés sur le cadre juridique et réglementaire en vigueur en RDC.

3. OBJECTIFS

3.1. Objectif global

L'objectif général de la mission est d'accompagner le Gouvernement dans la définition, la planification et la structuration opérationnelle d'un Système National d'Identification de la Population (SNIP), conforme aux Principes sur l'Identification pour un Développement Durable[1] et reposant sur une approche d'infrastructure publique numérique (DPI). [2]

La mission inclura également la réalisation d'un audit technique et organisationnel approfondi de l'Office National d'Identification de la Population (ONIP), en vue d'évaluer ses capacités actuelles, d'identifier les écarts par rapport aux exigences d'un SNIP moderne et interopérable, et de proposer une feuille de route de renforcement alignée sur la stratégie nationale d'identification.

Cela impliquera notamment :

i) de réaliser un état des lieux complet de l'écosystème de l'identité en RDC, incluant l'audit technique et organisationnel de l'ONIP, et de proposer des options adaptées pour la mise en place du SNIP ;

ii) d'élaborer une stratégie nationale intégrée assortie de feuilles de route opérationnelles pour :

- L'identification biométrique de la population sur l'ensemble du territoire national ;
- La constitution et la gestion du Fichier Général de la Population (FGP) ;
- La création de l'identité numérique et des services d'authentification ;
- Le renforcement institutionnel et organisationnel des acteurs clés, en particulier l'ONIP.

3.2. Objectifs spécifiques

Les objectifs spécifiques sont les suivants :

Volet A – Diagnostic global de l'écosystème de l'identité et audit ONIP

[1] https://www.idprinciples.org/
[2] https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031025172027713

- Réaliser un état des lieux complet de l'écosystème national de l'identité, incluant les dimensions institutionnelles, techniques, opérationnelles et de services ;
- Faire un état des lieux spécifique et détaillé de l'ONIP comprenant :
    - Audit technique des infrastructures, systèmes d'information, solutions biométriques, réseaux, cybersécurité, continuité d'activité et interopérabilité ;
    - Audit organisationnel couvrant la gouvernance, les processus métiers, la gestion des opérations d'enrôlement, la gestion des données, la maintenance des systèmes et la coordination interinstitutionnelle ;
    - Évaluation des ressources humaines, des compétences techniques, des mécanismes de formation et de transfert de connaissances ;
    - Analyse des modèles financiers et de durabilité opérationnelle ;
- Identifier les forces, faiblesses et besoins en matière de gouvernance et de coordination du secteur de l'identification ;
- Consulter l'ensemble des parties prenantes publiques et privées concernées afin d'harmoniser les visions et de définir une vision nationale intégrée du SNIP ;
- Évaluer le cadre institutionnel et les capacités des principaux acteurs et formuler des recommandations de réformes et de renforcement des capacités.

Volet B – Cadre juridique et institutionnel

- Réaliser une revue exhaustive du cadre juridique et réglementaire applicable à l'identification et à l'identité numérique ;
- Identifier les lacunes législatives notamment en matière de protection des données personnelles, identité numérique, signature électronique, preuves numériques, état civil, délégation de service public ;
- Élaborer des recommandations de réformes légales et réglementaires facilitant l'accès sécurisé au FGP et l'utilisation de l'identité numérique ;
- Définir le positionnement institutionnel optimal de l'ONIP dans l'architecture globale du SNIP.

Volet C – Architecture technique cible et normes

- Définir l'architecture cible du SNIP en tenant compte des résultats de l'audit technique de l'ONIP ;
- Concevoir les standards techniques couvrant :
    - Identification biométrique et biographique ;

    - Fichier Général de la Population ;
    - Carte d'Identité Nationale sécurisée ;
    - Services d'authentification et identité numérique ;
    - Interopérabilité avec registres sectoriels et services à fort impact (KYC, e-Santé, e-Tax, transferts sociaux, etc.) ;
- Définir les normes de cybersécurité et de protection des données (ISO 27001/27701, NIST, standards équivalents au RGPD) ;
- Proposer un cadre de confiance numérique (PKI / Trust Framework) aligné avec les autres initiatives nationales ;
- Proposer un modèle d'intégration et de consolidation des données biométriques existantes au niveau national.

Volet D – Stratégie SNIP et feuilles de route opérationnelles

- Élaborer le schéma directeur stratégique du SNIP ;
- Définir la feuille de route de transformation et de renforcement de l'ONIP, incluant :
    - Modernisation technique ;
    - Renforcement organisationnel ;
    - Optimisation des processus d'enrôlement et de gestion des identités ;
    - Renforcement cybersécurité et protection des données ;
- Élaborer les feuilles de route d'opérationnalisation couvrant :
    - Phasage de l'enrôlement national ;
    - Migration et consolidation des données existantes ;
    - Production et distribution des titres d'identité ;
    - Déploiement des services d'authentification ;
    - Intégration progressive des registres sectoriels ;
    - Dimensionnement des infrastructures (Cloud souverain, DC, réseaux GovNet, etc.).

Volet E – Interopérabilité et gouvernance des données

- Définir le cadre national d'interopérabilité du FGP ;
- Définir les modalités d'hébergement souverain sécurisé ;
- Définir les mécanismes d'interconnexion avec les services publics et privés ;
- Intégrer les exigences de biométrie révocable, identité numérique et signature électronique.

Volet F – Renforcement des capacités et gestion du changement

- Élaborer un plan national de renforcement des capacités ;

- Élaborer un plan spécifique de renforcement institutionnel et technique de l'ONIP ;
- Définir la stratégie nationale de conduite du changement.

Volet G – Livrables techniques finaux

Le cabinet devra produire notamment :

- Rapport d'audit technique et organisationnel de l'ONIP ;
- Stratégie nationale intégrée de l'identification et de l'identité numérique ;
- Schéma Directeur SNIP détaillé + synthèse exécutive ;
- Plan d'action triennal et budget détaillé ;
- Feuilles de route d'opérationnalisation ;
- Cadre national d'interopérabilité du FGP ;
- Recommandations réglementaires ;
- DAO / Cahiers des charges types ;
- Note stratégique sur le financement et la durabilité.

4. RÉSULTATS ATTENDUS

1. Alignement stratégique national et rationalisation des investissements

- Un schéma directeur du SNIP offrira une feuille de route consolidée permettant d'éviter la duplication des investissements publics, d'aligner les projets relatifs à l'ONIP, à l'état civil (CRVS), au système électoral, aux services financiers numériques et aux services publics digitaux.
- Le schéma directeur définira des standards d'interopérabilité compatibles avec les cadres africains (AU-ID) et internationaux (ISO, ICAO, MOSIP, OSIA).
- Le consultant devra évaluer l'ensemble des systèmes fonctionnels nationaux liés à l'identification, notamment :
    - Les systèmes collectant des données biométriques ;
    - Les infrastructures technologiques utilisées ;
    - Les cibles de population couvertes ;
    - Les coûts et sources de financement ;
    - Les modèles d'implémentation (public, PPP, BOT, etc.) ;
    - Les contraintes d'interopérabilité.
- L'analyse devra inclure également les systèmes financés par les partenaires techniques et financiers (ex. programmes réfugiés, projets sectoriels, initiatives provinciales), afin d'estimer le coût global supporté par l'État pour des systèmes non interopérables.

2. Diagnostic approfondi et feuille de transformation de l'ONIP

- Production d'un rapport d'audit technique et organisationnel complet de l'ONIP couvrant :
    - L'architecture technique existante (infrastructures, systèmes biométriques, data centers, réseaux, cybersécurité, continuité d'activité) ;
    - Les processus opérationnels (enrôlement, gestion des données, production de titres, maintenance des systèmes) ;
    - La gouvernance institutionnelle et la coordination interinstitutionnelle ;
    - Les capacités humaines et organisationnelles ;
    - La viabilité financière et les modèles économiques actuels.
- Identification claire des écarts entre les capacités actuelles de l'ONIP et les exigences d'un SNIP conforme aux standards internationaux.
- Élaboration d'une feuille de route de transformation de l'ONIP intégrant :
    - Modernisation technique ;
    - Renforcement organisationnel ;
    - Renforcement cybersécurité et protection des données ;
    - Plan de développement des compétences ;
    - Stratégie de durabilité financière.

3. Accélération de l'inclusion socio-économique

- Mise en place des bases d'un identifiant unique fiable facilitant :
    - L'inclusion financière (KYC simplifié, mobile money, microcrédit) ;
    - La protection sociale ciblée ;
    - L'accès aux services publics (santé, éducation, administration) ;
    - La participation électorale sécurisée.
- Définition de mécanismes optimisés d'enrôlement, d'authentification et de vérification réduisant les coûts d'accès aux services publics et privés.

4. Renforcement de la gouvernance, de la confiance numérique et de la cybersécurité

- Clarification des rôles institutionnels des acteurs clés :
    - Ministère de l'Intérieur, Ministère de l'Économie Numérique, Ministère de la Justice, ONIP, INS, CENI, provinces, agences sectorielles.
- Intégration des principes **privacy by design** conformément à la Loi 18/043 et aux standards internationaux (ISO 27701, ISO 29100).

- Définition d'un cadre national sécurisé de partage et d'interopérabilité des données.
- Contribution à la lutte contre :
    - Fraude documentaire ;
    - Usurpation d'identité ;
    - Cybermenaces liées aux données d'identité.

5. Optimisation des ressources publiques et mobilisation des partenaires

- Mise à disposition d'un schéma directeur crédible facilitant :
    - La mobilisation de financements concessionnels ;
    - L'investissement du secteur privé (opérateurs mobiles, fintech, identity service providers) ;
    - L'alignement des interventions des partenaires techniques et financiers.
- Définition :
    - Des coûts CAPEX / OPEX par composante ;
    - Des modèles PPP / BOT adaptés au contexte RDC ;
    - D'un modèle de soutenabilité financière du SNIP et des opérations ONIP.

6. Mise en place d'un cadre de suivi-évaluation et d'impact mesurable

- Élaboration d'un cadre logique complet comprenant :
    - Indicateurs d'enrôlement ;
    - Indicateurs d'authentification et d'usage ;
    - Indicateurs de couverture territoriale ;
    - Indicateurs de satisfaction citoyenne ;
    - Indicateurs de cybersécurité et de protection des données.
- Mise en place d'un dispositif de monitoring basé sur des tableaux de bord interopérables avec les systèmes statistiques nationaux et les systèmes de suivi du programme de transformation numérique.

7. Contribution à la construction de l'infrastructure publique numérique nationale

- Contribution à la mise en place des briques DPI nationales :
    - Identité numérique ;
    - Authentification ;
    - Interopérabilité ;
    - Partage sécurisé des données.

Official Use Only

- Alignement avec les initiatives nationales stratégiques :
    - Cloud souverain gouvernemental ;
    - GovNet ;
    - Plateformes de services publics numériques ;
    - Cadre national de cybersécurité.

8. Harmonisation avec les autres initiatives nationales et appuis techniques

Le consultant devra collaborer avec les autres cabinets ou partenaires intervenant dans les domaines :

- Identification ;
- État civil ;
- Services numériques publics ;
- Protection des données ;
- Cybersécurité.

Afin d'assurer :

- Une cohérence stratégique nationale ;
- L'harmonisation des recommandations techniques ;
- L'optimisation de l'utilisation des financements publics et des appuis extérieurs.

5. ACTIVITÉS PRINCIPALES

Plan de travail : activités clés et livrables attendus pour l'élaboration du Schéma Directeur du SNIP

Phase / Activités principales	Contenu des travaux	Livrables correspondants
0. Mobilisation et cadrage de la mission	• Réunion de lancement (Kick-off) • Validation méthodologie détaillée • Validation plan de travail • Revue documentaire initiale • Planification détaillée (Gantt, gouvernance projet, RACI) • Finalisation méthodologie d'audit ONIP	• **Rapport d'inception** • **Plan d'audit ONIP détaillé** • **Stratégie collecte données**
1. Diagnostic global de l'écosystème national de l'identité	• Inventaire institutionnel, technique et financier (ONIP, CRVS, CENI, INSS, DGI, etc.) • Cartographie systèmes biométriques existants • Enquêtes terrain et consultations nationales • Analyse offre / demande services d'identification • Analyse macro-juridique (préliminaire)	• **Rapport diagnostic écosystème** • Cartographie systèmes nationaux • **Base de données des acteurs et systèmes**
2. Audit technique, organisationnel et financier de l'ONIP	**Audit technique** • Infrastructures IT et biométriques • Systèmes enrôlement et gestion identité • Cybersécurité • Continuité d'activité • Interopérabilité • Intégration Cloud souverain / GovNet	• Rapport complet Audit ONIP • Feuille transformation ONIP

Phase / Activités principales	Contenu des travaux	Livrables correspondants
	Audit organisationnel • Gouvernance ONIP • Processus métiers • Organisation opérationnelle • Coordination interinstitutionnelle • Capacités RH **Audit financier** • Analyse CAPEX / OPEX actuels • Coût unitaire enrôlement • Modèle économique • Soutenabilité financière **Transformation ONIP** • Gap analysis • Plan transformation 3–5 ans • Plan modernisation technique • Plan renforcement institutionnel	
3. Vision stratégique SNIP et gouvernance cible	• Vision nationale SNIP • Principes directeurs DPI / ID4D • Modèle gouvernance SNIP • Positionnement cible ONIP	• Note Vision SNIP • Cadre gouvernance validé

Official Use Only

Phase / Activités principales	Contenu des travaux	Livrables correspondants
4. Architecture cible SNIP et normes techniques	• Architecture SNIP complète • Architecture biométrie • Architecture identité numérique • Architecture interopérabilité • Normes cybersécurité • Trust Framework / PKI • Hébergement souverain	• Architecture SNIP détaillée • Référentiel normes et cybersécurité
5. Schéma Directeur SNIP et feuilles de route opérationnelles	• Axes stratégiques SNIP • Séquencement déploiement national • Plan transformation ONIP • Plan d'enrôlement national • Migration données • Dimensionnement infrastructures et RH • Plan action budgété	• Schéma Directeur SNIP • Feuilles de route opérationnelles
6. Cadre juridique et réglementaire	• Analyse écarts législatifs • Propositions réformes • Textes réglementaires types • Cadre accès électronique sécurisé FGP	• Rapport juridique • Projets textes réglementaires
7. Modèle économique et durabilité	• Estimation CAPEX / OPEX SNIP • Modèles financement (Budget / Bailleurs / PPP) • Analyse soutenabilité • Modèle économique ONIP post-transformation	• Modèle économique SNIP • Note financement durable
8. Cadre national d'interopérabilité	• Cadre interopérabilité FGP • Modélisation échanges données	• Cadre interopérabilité national • Spécifications API

Phase / Activités principales	Contenu des travaux	Livrables correspondants
	• APIs et registre maître • Intégration biométrie révocable et signature numérique	
9. Renforcement des capacités et conduite du changement	• Analyse besoins compétences • Plan formation ONIP et institutions • Stratégie changement national	• Plan renforcement capacités • Plan conduite changement
10. Suivi-évaluation et gestion des risques	• Cadre M&E SNIP • Indicateurs ODD 16.9 • Matrice risques techniques / juridiques / financiers / sociaux	• Cadre M&E SNIP • Matrice risques et plan mitigation
11. Documentation de passation des marchés	• DAO et CCTP types : – Biométrie – Enrôlement – CIN – Identité numérique – Intégration CRVS – PKI / cybersécurité / SOC	• DAO et CCTP prêts publication
12. Rapport final et clôture mission	• Consolidation livrables • Atelier restitution • Transfert de connaissances	• Rapport final mission • Synthèse exécutive • Plan action triennal budgété

Remarques organisationnelles

- **Calendrier indicatif** : 10 mois, avec points d'arrêt de validation à la fin des Phases 1, 3, 4 et 10. L'UGP facilitera l'organisation des différents ateliers de validation et l'intégration de toutes les parties prenantes concernées.
- **Méthodologie** : approche participative, alignée sur les Digital Public Goods et les principes MOSIP/Open-Source pour maximiser la réutilisabilité et l'indépendance technologique. Le consultant devra mener des consultations approfondies avec les différentes parties prenantes au niveau national et avec un échantillon représentatif de parties prenantes au niveau décentralisé afin d'élaborer cette stratégie et ce plan directeur. À la fin, il doit proposer une approche dans sa feuille de route pour bâtir et assurer une collaboration entre le gouvernement (« whole-of-government approach »), et toutes les instances du gouvernement impliquées.
  Le consultant est également encouragé à intégrer des critères d'inclusion et de diversité dans l'élaboration de ce plan directeur, étant donné que les systèmes d'identification sont construits sur des principes d'inclusion.
  Le consultant doit aligner la stratégie et le plan directeur sur les principes d'identification pour le développement durable (ID4D) de la Banque mondiale.
- **Développement d'un consensus national** : Le consultant préparera et animera des ateliers nationaux clés afin de sensibiliser, harmoniser, réorganiser et valider la vision et l'approche du gouvernement en matière de systèmes d'identification.
- **Transfert de compétences** : prévu tout au long de la mission (co-working, formations « train-the-trainer », documentation).
  Ce découpage garantit que chaque objectif spécifique se traduit par un **ensemble clair d'activités structurées et de livrables vérifiables**, offrant aux parties prenantes une visibilité complète sur la progression vers un SNIP pérenne, sécurisé et inclusif.

Official Use Only

6. LIVRABLES, CALENDRIER INDICATIF ET MODALITÉS DE VALIDATION.

Le cabinet devra produire l'ensemble des livrables nécessaires à l'élaboration de la stratégie intégrée de l'identification, du schéma directeur du SNIP, ainsi que des résultats de l'audit technique et organisationnel de l'ONIP.

Tous les livrables devront être fournis en français (et en anglais si requis), en version électronique modifiable et en version PDF.

6.1. Principes généraux

Les livrables devront :

- Être conformes aux standards internationaux en matière d'identification numérique et de DPI ;
- Être alignés avec le cadre juridique et réglementaire de la RDC ;
- Intégrer les résultats de l'audit ONIP dans les recommandations stratégiques ;
- Être validés par le Comité technique du projet et les parties prenantes désignées ;
- Être compatibles avec une utilisation ultérieure pour la préparation des DAO de mise en œuvre.

6.2. Liste détaillée des livrables

Livrable 1 – Rapport de démarrage (Inception Report)

Contenu minimum :

- Compréhension détaillée de la mission ;
- Méthodologie détaillée ;
- Plan de travail ;
- Plan de consultation des parties prenantes ;
- Méthodologie détaillée d'audit ONIP (technique + organisationnel + financier) ;
- Plan de gestion des risques.

Délai indicatif : 3 à 4 semaines après démarrage.

Livrable 2 – Rapport de diagnostic de l'écosystème national de l'identification

Contenu minimum :

- Cartographie des systèmes existants ;

- Analyse des coûts globaux des systèmes actuels ;
- Analyse de la fragmentation des données ;
- Analyse des initiatives financées par les bailleurs ;
- Analyse de l'offre et de la demande des services d'identification.

Délai indicatif : Mois 2.

Livrable 3 – Rapport d'audit technique et organisationnel de l'ONIP

Contenu minimum :

Audit technique

- Analyse infrastructures IT et biométriques
- Analyse cybersécurité
- Analyse interopérabilité
- Analyse continuité d'activité
- Analyse intégration Cloud souverain / GovNet

Audit organisationnel

- Gouvernance ONIP
- Processus métiers
- Capacités RH
- Organisation opérationnelle

Audit financier

- Analyse coûts opérationnels
- Analyse soutenabilité
- Analyse modèles économiques

Recommandations

- Gap analysis complète
- Feuille de transformation ONIP 3–5 ans

Délai indicatif : Mois 3 – 4.

Livrable 4 – Rapport cadre juridique et institutionnel

Contenu minimum :

- Analyse cadre légal existant
- Identification des lacunes
- Propositions de réformes
- Recommandations positionnement institutionnel SNIP / ONIP

Délai indicatif : Mois 4.

Livrable 5 – Architecture cible SNIP et cadre d'interopérabilité

Contenu minimum :

- Architecture fonctionnelle SNIP
- Architecture technique cible
- Architecture d'interopérabilité
- Cadre cybersécurité
- Trust Framework / PKI
- Modèle consolidation biométrie

Délai indicatif : Mois 5.

Livrable 6 – Stratégie nationale intégrée de l'identification

Contenu minimum :

- Vision stratégique
- Piliers stratégiques
- Modèle gouvernance SNIP
- Modèle transformation ONIP
- Modèle financement global

Délai indicatif : Mois 6.

Livrable 7 – Schéma Directeur détaillé du SNIP

- Plan directeur global
- Phasage déploiement
- Dimensionnement infrastructures
- Plan transformation ONIP
- Plan cybersécurité

Délai indicatif : Mois 7.

Livrable 8 – Feuilles de route opérationnelles

- Feuille d'enrôlement national
- Feuille migration données

- Feuille intégration registres sectoriels
- Feuille déploiement identité numérique
- Feuille transformation ONIP

Délai indicatif : Mois 8.

Livrable 9 – Plan d'action triennal budgétisé

- Plan opérationnel détaillé
- CAPEX / OPEX
- Modèles financement
- Analyse soutenabilité

Délai indicatif : Mois 8 – 9.

Livrable 10 – Dossiers techniques pré-DAO

- Spécifications techniques types
- Cahiers des charges types
- Recommandations structuration lots

Délai indicatif : Mois 9.

Livrable 11 – Rapport final consolidé

- Consolidation de tous les livrables
- Synthèse exécutive
- Présentation officielle gouvernement

Délai indicatif : Fin mission.

6.3. Modalités de validation

Chaque livrable devra :

- Être présenté lors d'un atelier technique de validation ;
- Être soumis pour commentaires ;
- Être révisé et soumis en version finale.

6.4. Calendrier indicatif global

Durée indicative totale : **10 mois**

6.5. Logique jalons paiement

N°	Livrables	Echéance	Pourcentage
1	**Livrable 1 – Rapport de démarrage**	3 à 4 semaines après démarrage	10 %
2	**Livrable 2 – Rapport de diagnostic de l'écosystème national de l'identification**	2 mois	15 %
3	**Livrable 3 – Rapport d'audit technique et organisationnel de l'ONIP**	Mois 3 – 4.	20 %
4	**Livrable 4 – Rapport cadre juridique et institutionnel** **Livrable 5 – Architecture cible SNIP et cadre d'interopérabilité**	Mois 4.	15 %
5	**Livrable 6 – Stratégie nationale intégrée de l'identification** **Livrable 7 – Schéma Directeur détaillé du SNIP**	Mois 7	20 %
6	Feuilles route + budget + DAO : **Livrable 8 – Feuilles de route opérationnelles** **Livrable 9 – Plan d'action triennal budgétisé** **Livrable 10 – Dossiers techniques pré-DAO**	Mois 8-9	15 %
7	Rapport final **Livrable 11 – Rapport final consolidé**	Mois 9	5 %

7. MÉTHODOLOGIE DE MISE EN ŒUVRE DE LA MISSION

Le cabinet devra proposer une méthodologie rigoureuse, structurée, participative et orientée vers la mise en œuvre opérationnelle, permettant d'assurer la qualité technique des livrables, l'appropriation par les parties prenantes nationales et l'alignement avec les standards internationaux en matière d'identification numérique et d'infrastructure publique numérique (DPI).

Official Use Only

7.1. Principes méthodologiques généraux

La méthodologie proposée devra être basée sur les principes suivants :

- Approche centrée sur les besoins du gouvernement de la RDC ;
- Alignement avec les Principes pour l'Identification pour le Développement Durable (ID4D) ;
- Approche DPI (Digital Public Infrastructure) ;
- Approche Whole-of-Government ;
- Approche basée sur les risques ;
- Approche orientée mise en œuvre et durabilité ;
- Approche participative et inclusive.

7.2. Approche méthodologique globale

La mission devra être conduite selon une approche en plusieurs niveaux :

Niveau 1 – Analyse stratégique et institutionnelle

- Analyse des politiques publiques existantes ;
- Analyse des stratégies nationales numériques ;
- Analyse du positionnement institutionnel du SNIP et de l'ONIP ;
- Analyse des initiatives DPI nationales.

Niveau 2 – Analyse technique et opérationnelle

- Analyse des architectures existantes ;
- Analyse des systèmes biométriques ;
- Analyse des systèmes d'état civil ;
- Analyse des systèmes sectoriels ;
- Analyse cybersécurité ;
- Analyse infrastructures (Data Centers, Cloud souverain, GovNet).

Niveau 3 – Analyse économique et de durabilité

- Analyse coûts CAPEX / OPEX ;
- Analyse modèles économiques ;
- Analyse options PPP / BOT ;
- Analyse de la soutenabilité financière.

7.3. Méthodologie spécifique d'audit technique et organisationnel de l'ONIP

Le cabinet devra proposer une méthodologie d'audit conforme aux standards internationaux IT Audit, Cybersecurity Audit et Institutional Assessment.

7.3.1. Audit technique

Basé sur :

- Référentiels ISO 27001 / 27701 ;
- Framework NIST Cybersecurity ;
- Bonnes pratiques internationales d'identité numérique.

Méthodes attendues :

- Revue documentaire technique ;
- Analyse architecture systèmes ;
- Tests de cohérence et maturité ;
- Interview techniques ;
- Visites sites techniques ;
- Analyse sécurité et continuité.

7.3.2. Audit organisationnel

Basé sur :

- Institutional capacity assessment ;
- Business process analysis ;
- Governance assessment.

Méthodes attendues :

- Interviews direction ONIP ;
- Analyse organigrammes ;
- Analyse processus métiers ;
- Analyse coordination interinstitutionnelle ;
- Analyse de gestion RH et compétences.

7.3.3. Audit financier et durabilité

Méthodes attendues :

- Analyse coûts historiques ;
- Analyse coûts unitaires enrôlement ;
- Analyse modèles financement ;
- Analyse de la viabilité à long terme.

7.4. Approche de consultation et d'engagement des parties prenantes

Le cabinet devra :

- Cartographier les parties prenantes ;
- Organiser ateliers techniques sectoriels ;
- Organiser ateliers validation multi-acteurs ;
- Mettre en place un mécanisme de feedback continu.

7.5. Approche de conception de la stratégie SNIP et du Schéma Directeur

Le cabinet devra adopter une approche :

- Evidence-based ;
- Data-driven ;
- Alignée standards internationaux ;
- Adaptée au contexte RDC.

7.6. Approche de conception des feuilles de route opérationnelles

Les feuilles de route devront être :

- Réalistes ;
- Budgétisées ;
- Priorisées ;
- Alignées capacités ONIP et écosystème national ;
- Alignées capacités infrastructures nationales (Cloud, GovNet, DC).

7.7. Approche de transfert de compétences

Le cabinet devra :

- Associer étroitement les équipes nationales ;
- Produire guides techniques ;
- Former équipes ONIP et ministères ;
- Assurer le transfert méthodologique.

7.8. Approche assurance qualité

Le cabinet devra mettre en place :

- Revue interne qualité ;
- Validation technique progressive ;
- Validation parties prenantes ;
- Validation institutionnelle finale.

7.9. Gestion des risques

Le cabinet devra proposer un plan de gestion couvrant :

- Risques institutionnels ;
- Risques techniques ;
- Risques cybersécurité ;
- Risques financiers ;
- Risques d'adoption des utilisateurs.

7.10. Exigences en matière de reporting

Le cabinet devra :

- Produire rapports périodiques ;
- Produire notes techniques si requis ;
- Participer réunions de suivi ;
- Maintenir une communication continue avec UGPTN.

8. PROFIL DU CABINET ET DES EXPERTS CLÉS

8.1. Profil général du cabinet

Le cabinet devra être une firme de conseil, internationale ou nationale, disposant d'une expérience avérée d'au moins dix (10) ans dans la conception, la planification ou la mise en œuvre de systèmes nationaux d'identification, d'infrastructures publiques numériques (DPI) ou de systèmes d'information gouvernementaux à grande échelle.

Le cabinet devra démontrer :

- Une expérience avérée dans au moins **trois (3) missions similaires (prestations de même nature, de complexité semblable et de volume financier similaire)** au cours des dix (10) dernières années ;
- Une expérience dans la conception ou l'accompagnement de systèmes d'identification biométrique nationale, identité numérique ou registres de population ;
- Une expérience en matière d'audit technique de systèmes d'information critiques ;
- Une expérience en matière d'analyse institutionnelle et organisationnelle d'institutions publiques ;
- Une expérience dans des projets financés par des partenaires techniques et financiers internationaux (Banque mondiale, BAD, UE, etc.) constituera un avantage ;
- Une expérience en Afrique subsaharienne ou dans des contextes institutionnels comparables constituera un atout majeur.

8.2. Domaines d'expertise technique requis du cabinet

Le cabinet devra démontrer une expertise dans les domaines suivants :

- Systèmes nationaux d'identification et registres de population ;
- Identification biométrique et systèmes d'enrôlement ;
- Identité numérique et authentification ;
- DPI (Digital Public Infrastructure) ; Interopérabilité et partage de données gouvernementales ;
- Cybersécurité et protection des données ;
- Gouvernance des données ;
- Transformation institutionnelle et conduite du changement ;
- Modélisation financière de systèmes publics numériques.

8.3. Composition minimale de l'équipe clé

Le cabinet devra proposer une équipe pluridisciplinaire comprenant au minimum les experts clés suivants.

8.3.1. Chef de mission / Expert principal Identification & DPI

Profil minimum :

- Diplôme supérieur (Master ou plus) en informatique, ingénierie, systèmes d'information, politiques publiques numériques ou équivalent ;
- Minimum 12 ans d'expérience professionnelle ;
- Expérience dans au moins deux projets nationaux d'identification ou d'identité numérique ;
- Expérience dans la gestion de missions complexes multi-acteurs ;
- Expérience de projets financés par des bailleurs internationaux souhaitée.

8.3.2. Expert audit technique systèmes d'identification et infrastructures IT

- Diplôme supérieur (Master ou plus) en informatique, ingénierie, systèmes d'information ou équivalent ;
- Minimum 10 ans d'expérience ;
- Expérience audit systèmes biométriques ou identity platforms ;
- Expérience audit cybersécurité ;
- Expérience audit infrastructures critiques.

8.3.3. Expert transformation institutionnelle et audit organisationnel

- Diplôme supérieur (Master ou plus) en administration publique, sciences politiques, économie / développement, gestion / management des organisations, droit public ou institutionnel, audit / contrôle de gestion, ingénierie organisationnelle, transformation digitale / gouvernance IT ou équivalent ;

- Minimum 10 ans d'expérience ;
- Expérience réforme institutions publiques ;
- Expérience analyse processus métiers ;
- Expérience gouvernance institutions publiques.

8.3.4. Expert architecture systèmes d'identification et interopérabilité

- Diplôme supérieur (master ou plus) en informatique / génie logiciel, systèmes d'information, télécommunications, cybersécurité, data engineering / architecture IT ou équivalent ;
- Minimum 10 ans d'expérience ;
- Expérience architecture identity stack ;
- Expérience interopérabilité gouvernementale ;
- Expérience API Government Platforms.

8.3.5. Expert cybersécurité et protection des données

- Diplôme supérieur (master ou plus) en informatique / génie logiciel, systèmes d'information, télécommunications, cybersécurité, data engineering / architecture IT ou équivalent ; Minimum 8 à 10 ans d'expérience ;
- Expérience ISO 27001 / NIST ;
- Expérience systèmes d'identité ou de données sensibles.

8.3.6. Expert juridique – protection des données, identité numérique et confiance numérique

- Diplôme supérieur (master ou plus) en droit du numérique / droit des TIC, droit public / administratif, protection des données personnelles, droit des télécommunications, droit des contrats / droit international ou équivalent ;
- Minimum 8 ans d'expérience ;
- Expérience droit numérique ;
- Expérience protection données ;
- Expérience réglementation identité numérique.

8.3.7. Expert modèle économique et durabilité financière

- Diplôme supérieur (master ou plus) en économie (publique, développement, industrielle), finance (corporate finance, finance publique), gestion / stratégie, politiques publiques, Business administration (MBA) ou équivalent ;
- Minimum 8 ans d'expérience ;
- Expérience modélisation CAPEX/OPEX systèmes numériques publics ;

- Expérience PPP / BOT ;
- Expérience en financement de projets publics numériques.

8.3.8. Expert renforcement des capacités et conduite du changement

- Diplôme supérieur (master ou plus) en ressources humaines / gestion des organisations, psychologie du travail / sociologie des organisations, administration publique, management / stratégie, sciences de l'éducation / ingénierie de formation ou équivalent ;
- Minimum 8 ans d'expérience ;
- Expérience programmes formation secteur public ;
- Expérience de conduite du changement de la transformation numérique.

8.4. Autres personnels

- Expert biométrie avancée ;
- Expert CRVS / état civil ;
- Expert data governance ;
- Expert infrastructures cloud souverain / data centers ;
- Expert GovTech services publics numériques.

8.5. Exigences en matière de disponibilité

Le cabinet devra garantir :

- Disponibilité du Chef de mission pendant toute la mission ;
- Mobilisation effective des experts clés selon le planning ;
- Stabilité de l'équipe (remplacements soumis à validation).

8.6. Transfert de compétences

Le cabinet devra démontrer sa capacité à :

- Travailler étroitement avec les équipes nationales ;
- Former les équipes ONIP et institutions partenaires ;
- Produire une documentation technique transférable.

8.7. Langue de travail

- Français obligatoire ;
- Anglais souhaité.

Official Use Only

9. ORGANISATION, GOUVERNANCE ET SUPERVISION DE LA MISSION

9.1. Autorité contractante et institution bénéficiaire

La mission sera mise en œuvre dans le cadre du Projet de Transformation Numérique (PTN).

L'autorité contractante est l'Unité de Gestion du Projet de Transformation Numérique (UGPTN).

L'institution bénéficiaire principale est le Gouvernement de la République Démocratique du Congo, à travers les institutions en charge de l'identification de la population, notamment l'Office National d'Identification de la Population (ONIP), ainsi que les ministères et institutions concernés par l'écosystème de l'identification et de l'identité numérique.

9.2. Supervision technique de la mission

La supervision technique sera assurée par :

- Le Responsable de la Composante 2 du projet ;
- L'équipe technique de l'UGPTN ;
- Le Comité technique multisectoriel qui sera mis en place pour le suivi de la mission.

La supervision technique couvrira notamment :

- Validation méthodologique ;
- Validation technique des livrables ;
- Coordination avec les autres activités du projet ;
- Suivi de la qualité technique des travaux du cabinet.

9.3. Mécanisme de gouvernance de la mission

Un dispositif de gouvernance sera mis en place comprenant :

Comité de Pilotage (COPIL)

Rôle :

- Orientation stratégique ;
- Arbitrage des décisions majeures ;
- Validation des livrables stratégiques ;

- Facilitation de la coordination interinstitutionnelle.

Comité Technique

Rôle :

- Suivi opérationnel de la mission ;
- Validation technique intermédiaire des livrables ;
- Appui technique au cabinet ;
- Coordination technique interinstitutionnelle.

Points focaux institutionnels

Chaque institution clé impliquée dans l'écosystème SNIP désignera un point focal chargé :

- De faciliter l'accès aux données ;
- De coordonner la participation aux ateliers ;
- De faciliter les échanges techniques avec le cabinet.

9.4. Coordination spécifique avec l'ONIP (audit ONIP)

Compte tenu du rôle stratégique de l'ONIP, un mécanisme spécifique de coordination sera mis en place pour l'audit technique et organisationnel, incluant :

- Désignation d'un point focal ONIP ;
- Organisation d'ateliers techniques dédiés à l'ONIP ;
- Accès encadré aux systèmes, données et infrastructures ;
- Organisation de séances de restitution progressive.

9.5. Coordination avec les partenaires techniques et financiers

Le cabinet devra collaborer avec les partenaires techniques et financiers intervenant dans les domaines :

- Identification ;
- État civil ;
- DPI ;
- Cybersécurité ;
- Protection des données.

Le cabinet devra participer aux réunions de coordination si requis.

9.6. Modalités de validation des livrables

Chaque livrable devra suivre le processus suivant :

1. Soumission version provisoire ;
2. Revue technique UGPTN ;
3. Revue Comité technique ;
4. Atelier validation si nécessaire ;
5. Soumission version finale.

9.7. Organisation des réunions de suivi

Le cabinet devra participer aux réunions suivantes :

- Réunion de lancement ;
- Réunions techniques périodiques ;
- Réunions de revue des livrables ;
- Ateliers de validation ;
- Réunion de clôture de mission.

9.8. Exigences en matière de reporting

Le cabinet devra produire :

- Rapports d'avancement mensuels ;
- Notes techniques ad hoc si requis ;
- Rapports de mission terrain ;
- Rapports de risques si nécessaire.

9.9. Gestion des risques institutionnels et opérationnels

Le cabinet devra :

- Identifier les risques institutionnels ;
- Identifier les risques techniques ;
- Identifier les risques liés aux données sensibles ;
- Proposer des mesures d'atténuation.

Official Use Only

9.10. Transfert de compétences et appropriation nationale

Le cabinet devra :

- Associer les équipes nationales aux travaux ;
- Assurer un transfert progressif de compétences ;
- Produire guides et documentation technique ;
- Appuyer la montée en compétence des équipes ONIP.

9.11. Clôture de la mission

La mission sera considérée comme clôturée après :

- Validation du rapport final ;
- Organisation de l'atelier de restitution finale ;
- Transmission de tous les livrables et données associées.

Official Use Only

10. MODALITES DE REPORTING

Le consultant sera engagé par l'UGP, qui gérera le paiement et la validation des livrables. Tous les livrables doivent être soumis au Coordinateur de l'UGP. Des copies de tous les livrables seront également fournies à la Banque mondiale. Des représentants de l'initiative sur l'Identification pour le Développement (ID4D) de la Banque mondiale devront également être engagés lors des échanges techniques.

Un comité technique sera chargé d'examiner chaque livrable et disposera d'un délai d'une (1) semaine pour fournir des commentaires/valider chaque livrable. Sur demande, le consultant pourra également être tenu de présenter les livrables oralement [en personne ou virtuellement] aux parties prenantes concernées afin de permettre la formulation des commentaires et la validation. Les commentaires seront pris en compte dans la version finale soumise pour paiement.

Le consultant devra traiter tous les documents et communications dans le cadre de cet engagement de manière confidentielle.

11. PARTIES PRENANTES

Les principaux bénéficiaires de cette mission seront l'Office National de l'Identification de la Population (ONIP), le ministère de l'Intérieur et de la Sécurité (MIS) et le ministère de l'Économie Numérique (MEN). Toutefois, le consultant sera également tenu de consulter les parties prenantes suivantes concernées par la mission du côté du gouvernement : Agence pour le Développement du Numérique au sein de la Présidence, le Collège PTNTIC de la Présidence, Primature, l'Autorité de régulation de la poste et des télécommunications du Congo (ARPTC), le ministère de l'Intérieur et le Conseil National de la Cyberdéfense. Le gouvernement mettra en place un comité/commission consultatif réunissant toutes les institutions impliquées, pour lequel cette mission devrait également viser à impliquer la commission au maximum, afin de renforcer ses capacités, et qui sera chargé de définir et de partager la vision et les ambitions du gouvernement.

Tout au long de l'engagement, le consultant se coordonnera avec d'autres consultants travaillant sur les réformes juridiques. Par exemple, un consultant est en train d'être recruté pour l'élaboration des mesures d'application de la loi sur les télécommunications, financé par un autre projet de la Banque mondiale. En outre, un consultant est en train d'être recruté pour faciliter l'élaboration de feuilles de route pour l'identification numérique et l'enregistrement civil, qui comprend une analyse juridique connexe.

12. RESPONSABILITÉS DU CLIENT

Le gouvernement fournira, dans la mesure de ses moyens, les éléments suivants :

- Toute la documentation jugée pertinentes pour la réalisation ou l'information de la mission et l'accomplissement des tâches identifiées, dont il dispose. Cela comprend par exemple les documents politiques clés et les textes juridiques.
- L'accès aux principaux responsables des ministères/agences/départements concernés et autres entités officielles pertinentes, le cas échéant.
- Faciliter la coopération avec d'autres organisations, dont les activités et les programmes peuvent être considérés comme pertinents pour la mission. Cela inclut les autres cabinets travaillants sur des missions liées, comme indiqué ci-dessus.
- Le couts et l'organisation logistique liée à l'organisation des consultations/ateliers et à l'identification des personnes à former, en étroite collaboration avec le consultant.