



PROJET DE TRANSFORMATION NUMERIQUE « PTN »

PROJET N° P180495

ZR-UGP - PTN-527465-CS-QCBS

**TERMES DE RÉFÉRENCE POUR LE RECRUTEMENT D'UN
CABINET (FIRME) POUR UNE ASSISTANCE TECHNIQUE DANS
L'ÉTUDE DE DIMENSIONNEMENT DU RÉSEAU GOVNET EN
RÉPUBLIQUE DÉMOCRATIQUE DU CONGO**

Juin 2026

TABLES DES MATIERES

1.	CONTEXTE ET JUSTIFICATION	2
1.1.	Contexte	2
1.2.	Description du Projet d'Appui à Transformation Numérique de la RDC.....	2
1.3.	Les composantes du projet	3
1.4.	Portée géographique du projet	3
1.5.	Justification de la mission.....	4
2.	OBJECTIFS DE LA MISSION	5
2.1.	Objectif global	5
2.2.	Objectifs spécifiques.....	6
3.	PORTEE DE L'ETUDE / ACTIVITES A REALISER.....	Erreur ! Signet non défini.
4.	RESULTAT ATTENDUS.....	11
5.	LIVRABLES ATTENDUS	12
6.	PROFIL DU CABINET ET PERSONNEL CLE.....	13
7.	METHODOLOGIE ET DELAIS	17
8.	MODALITE DE SOUMISSION.....	18

1. CONTEXTE ET JUSTIFICATION

1.1. Contexte

Le gouvernement de la RDC a sollicité et obtenu l'appui du Groupe de la Banque Mondiale (GBM) et de l'Agence Française de Développement (AFD) pour le financement de la mise en œuvre du Projet de Transformation Numérique de la RDC, prévu pour être mis en œuvre sur une période de cinq ans.

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

Le taux de pénétration du haut débit s'élève actuellement à seulement 15,4 pour cent, sur la base d'abonnements à haut débit uniques¹ et les réseaux mobiles à large bande existants ne couvrent qu'environ la moitié de la population, avec des prix de détail du haut débit parmi les plus élevés d'Afrique. En outre, la prestation de services numériques est encore faible, avec peu de plateformes et de systèmes numérisés capables de faciliter l'efficacité des services publics et l'accès aux services par la population. Tous ces éléments, s'ils sont bien développés, peuvent contribuer et contribueront à créer d'immenses possibilités de création d'emploi, ainsi que de nombreuses possibilités d'entrepreneuriat pour les jeunes.

La connectivité gouvernementale en RDC se développe dans un environnement encore très contrasté. Plus de 70 % des zones rurales restent dépourvues d'accès fiable alors que la pénétration d'Internet mobile plafonnait à environ 30 % fin 2024, ce qui se reflète dans l'indice des infrastructures télécoms des Nations Unies (0,1591, bien en-deçà de la moyenne africaine de 0,45). Pour combler ce déficit, le gouvernement a lancé l'extension du backbone national à 50 000 km de fibre, négocié un câble sous-lacustre de 186 km entre Kigoma (Tanzanie) et Kalemie, et ouvert le marché satellitaire à Starlink le 2 mai 2025 pour desservir les territoires enclavés. Ces initiatives offrent une fenêtre inédite pour sécuriser, diversifier et fiabiliser les points d'accès du futur GovNet.

Dans cette dynamique, le dimensionnement du **GovNet** s'inscrit dans la mise en œuvre de la vision du *Plan national du numérique – Horizon 2025*, qui veut « faire du numérique un levier d'intégration, de bonne gouvernance, de croissance économique et de progrès social ». Le réseau devra constituer une dorsale haut débit, résiliente et sécurisée, interconnectant les 26 chefs-lieux provinciaux, les centres de données souverains et plus de 8 000 sites administratifs pour porter l'identité numérique, la signature électronique, l'interopérabilité et la cybersécurité des services publics. Son développement est adossé au Projet de Transformation Numérique de la RDC qui vise précisément à élargir l'accès inclusif à Internet et à renforcer les fondations de la fourniture de services numériques de l'État. Aboutir à un dimensionnement adéquat, c'est donc offrir à la RDC un réseau gouvernemental capable de réduire la fracture numérique, de stimuler l'innovation locale et de garantir aux citoyens un guichet unique fiable, accessible aussi bien depuis Kinshasa que dans les zones les plus reculées du pays.

Ainsi, le gouvernement a sollicité et obtenu un crédit auprès de la Banque mondiale (400 millions de dollars américains de l'IDA) et un co-financement de l'AFD (100 millions d'euros) pour financer la transformation numérique de la RDC. Le projet sera mis en œuvre sur une période de 5 ans, pour se terminer en 2029, et sera géré par une unité de gestion du projet dédiée.

1.2. Description du Projet d'Appui à Transformation Numérique de la RDC

Le PTN est conçu pour accroître l'accès à une connectivité haut débit abordable et de haute qualité, ainsi qu'à des services et solutions numériques à fort impact et en demande et développer des

¹ GSMA, 2022, Market Intelligence.

compétences numériques pertinentes pour l'industrie. L'objectif de développement du projet est d'améliorer l'accès à l'internet et aux services numériques en RDC et de favoriser leur utilisation par tous.

Pour ce faire, le PTN investira dans (i) l'infrastructure de connectivité numérique fondamentale nécessaire pour soutenir le mouvement vers l'accès numérique universel ; (ii) l'infrastructure publique numérique transversale (DPI) fondamentale requise pour faire évoluer les transactions numériques transactionnelles et à distance (dans les secteurs privé et public) ; prestation de services de manière rentable et sécurisée au niveau sectoriel ; (iii) renforcer la base de compétences numériques de la RDC pour garantir l'accès et l'utilisation productive de la technologie, tout en créant des liens avec des emplois numériques, et (iv) renforcer la capacité institutionnelle et la gouvernance nécessaires pour mener des initiatives connexes de manière concertée et intégrée.

1.3. Les composantes du projet

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

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

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

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

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

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

1.4. Portée géographique du projet

Les activités du projet seront mises en œuvre à l'échelle nationale, en se concentrant principalement sur les 10 provinces du Cadre de partenariat pays (CPF) entre la Banque mondiale et le

Gouvernement de la RDC, à savoir Kinshasa, Kwilu, Kongo-central, Kasai, Kasai Central, Kasai Oriental, Lomami, Nord-Kivu, Sud-Kivu et Ituri.

1.5. Justification de la mission

Dans le cadre du développement du **Plan Directeur e-Gouvernement**, le gouvernement de la République Démocratique du Congo (RDC) prévoit la mise en place d'un **réseau national sécurisé GovNet**. Ce réseau devra permettre d'interconnecter les administrations publiques sur l'ensemble du territoire national, notamment en capitalisant le droit inaliénable d'utilisation (IRU) de 25% de la capacité de fibre optique installée conformément à l'arrêté interministériel n°CAB/MIN/PT&NTIC/AKIM/KL/Kbs/057/2022 et n°CAB/MIN/FINANCES/154/2022 du 17 novembre 2022. Le **réseau national sécurisé GovNet** mis en place devrait ainsi assurer une **communication fiable, sécurisée et performante** entre les institutions gouvernementales.

Pour permettre au réseau national sécurisé GovNet de jouer son rôle, il devra être bien dimensionné (**réseau de transport des informations, services et des données**) et couvrir l'ensemble des **26 provinces, incluant la capitale Kinshasa**. Chaque chef-lieu provincial devra être doté d'un **ring de connectivité** auquel seront rattachés les différents sites administratifs. Ce réseau devra supporter **les services essentiels** tels que la vidéoconférence, la voix sur IP (VoIP), la messagerie électronique et d'autres applications e-Gouvernement.

En matière de connectivité gouvernementale, la RDC dispose d'un potentiel considérable, mais fait face à de nombreux défis. Le Gouvernement a déjà posé les bases d'un **GovNet** en reliant, par un backbone en fibre optique, 33 administrations à Kinshasa afin de leur fournir un accès Internet et de mutualiser certains services. Toutefois, la capacité haut débit reste insuffisante pour assurer des communications de qualité, l'hébergement fiable des registres, la fourniture de services numériques performants et le déploiement effectif d'un intranet gouvernemental.

Le réseau actuel exige donc une refonte complète afin d'offrir une connectivité robuste et homogène à l'ensemble des ministères, départements et agences (MDA), aux fonctionnaires ainsi qu'aux prestataires de première ligne. Les principaux écueils sont :

- Un financement limité ;
- L'absence d'une étude de faisabilité approfondie et d'une stratégie globale pour le GovNet ;
- Des performances et une fiabilité opérationnelle inégales ;
- Des LAN obsolètes, mal entretenus ou inexistantes dans de nombreux bâtiments publics.

Faute de bande passante suffisante ou de qualité, certaines MDA, qui en sont capables, souscrivent à leurs propres connexions auprès de fournisseurs privés, ce qui entraîne un coût global plus élevé, une fragmentation du réseau, une performance non optimisée et des failles de sécurité accrues. Les structures dépourvues de moyens, quant à elles, doivent freiner la numérisation de leurs processus et services.

Le gouvernement entend connecter toutes les administrations centrales, provinciales et locales — ministères, établissements publics, bureaux provinciaux, hôpitaux, agences territoriales, etc. — via un réseau unifié, animé par :

- Un accès mutualisé à la capacité Internet ;
- Un intranet gouvernemental sécurisé ;

- Des VPN pour les services critiques ;
- Des LAN modernisés ;
- Un centre d'exploitation réseau (NOC) ;
- Un modèle de gouvernance clair.

Parallèlement à la présente étude, le Gouvernement met en œuvre un projet distinct visant à établir un Centre Gouvernemental des Opérations de Cybersécurité (GovSOC). Compte tenu de l'état d'avancement de ce projet au moment de la réalisation de la présente mission, le cabinet devra analyser les synergies possibles entre GovNet et GovSOC et adapter la portée de ses recommandations relatives à la supervision de la sécurité en conséquence. Les propositions du cabinet devront être formulées en coordination avec l'UGPTN afin d'éviter les duplications et de garantir la complémentarité entre les deux initiatives.

Étant donné l'immensité du territoire congolais, cette extension doit s'appuyer sur une dorsale TIC fiable, intégrer les infrastructures privées existantes ou à venir, et être soutenue par un cadre de gouvernance, des normes techniques et opérationnelles solides, ainsi que des capacités renforcées de cybersécurité pour protéger le GovNet et les réseaux qui y sont raccordés.

La mission consiste à :

1. Évaluer en détail les besoins existants et futurs ;
2. Évaluer les besoins actuels et futurs (à moyen terme) ;
3. Estimer la capacité fibre optique utilisable par le gouvernement dans le cadre de l'arrêté interministériel ;
4. Proposer une stratégie d'utilisation de capacité fibre optique revenant de droit au gouvernement ;
5. Proposer un plan d'expansion phasé du GovNet vers les provinces ;
6. Définir un modèle adapté au contexte congolais pour son exploitation, son financement, sa gouvernance, la fourniture de services et la sécurisation de l'ensemble de l'écosystème.

Dans cette perspective, le gouvernement souhaite recruter un **cabinet spécialisé** pour mener une **étude technique et financière approfondie** afin de dimensionner et proposer un modèle optimal pour la mise en place et la pérennité de ce réseau.

2. OBJECTIFS DE LA MISSION

2.1. Objectif global

L'objectif général est de réaliser une étude de faisabilité complète de la mise en œuvre d'un intranet gouvernemental (GovNet) pour la RDC - couvrant le backbone national, les réseaux locaux (LAN) de tous les bâtiments publics, les centres de données, les couches de services et de sécurité associées, en garantissant l'interopérabilité avec les systèmes numériques déjà déployés - afin de :

- 1) Analyse de l'existant et des besoins futurs ;

- 2) Concevoir une architecture cible modulaire et évolutive qui prenne en compte la capacité fibre optique revenant de droit au gouvernement conformément à l'arrêté interministériel et assure la continuité, la performance et l'interopérabilité des services numériques gouvernementaux ;
- 3) Quantifier les coûts globaux d'investissement et d'exploitation (CAPEX / OPEX) pour l'infrastructure, les LAN et les services partagés ;
- 4) Identifier les contraintes techniques, économiques et réglementaires et proposer les mesures d'atténuation correspondantes ;
- 5) Définir un modèle de gouvernance clair pour le déploiement, l'exploitation et l'évolution de l'intranet ;
- 6) Elaborer l'ensemble des dossiers d'appels d'offres (DAO) nécessaires à la mise en œuvre progressive du réseau et des services associés.

2.2. Objectifs spécifiques

Les objectifs spécifiques sont :

1. Cartographie et évaluation de l'existant
 - Recenser :
 - le backbone fibre optique, les rings métropolitains, les faisceaux hertziens, les liaisons radio, VSAT et 4G/5G ;
 - les data centers, salles serveurs et locaux techniques ;
 - tout dispositif de supervision (NOC/SOC) déjà en place.
 - la capacité fibre optique utilisable par le gouvernement conformément à l'arrêté interministériel.
 - Mesurer leur état, leur capacité d'intégration et leur conformité aux normes de sécurité, d'énergie et de refroidissement.
2. Analyse des besoins fonctionnels et techniques
 - Quantifier, pour les administrations centrales, provinciales et locales :
 - la connectivité WAN, les LAN, le stockage de données, la continuité d'activité et les exigences de cybersécurité ;
 - les profils de trafic actuels et projetés, les SLA et les exigences de QoS.
3. Élaboration de scénarios d'architecture
 - Proposer plusieurs options technico-économiques (mix fibre propriétaire / liaisons louées, micro-ondes, satellite) ;
 - Détailler pour chaque option :
 - topologie, technologies et capacité évolutive ;
 - analyse avantages / inconvénients, CAPEX vs OPEX, délais de déploiement et risques.
4. Garantir l'interopérabilité technique et fonctionnelle avec les plateformes nationales existantes (e-Foncier, DGRAD, CNSSAP, e-Visa, etc.).
5. Règles de décision "déployer vs louer"
 - Définir des critères objectifs (distance, densité de trafic, coût du dernier kilomètre, durée d'amortissement, criticité des services, résilience souhaitée) pour choisir entre infrastructure propriétaire et location auprès d'ISP.
6. Dimensionnement détaillé
 - Calculer la capacité requise (bande passante, résilience, redondance) pour chaque segment ;
 - Dimensionner les LAN, les agrégations, les liens inter-DC, et les équipements actifs/passifs.
7. Services réseau et applicatifs à développer

- Spécifier la palette de services GovNet : VPN gouvernemental multisite, VoIP/visioconférence, DNS/PKI, messagerie sécurisée, supervision, authentification, services cloud internes, etc.
- 8. Supervision, maintenance et exploitation
 - Concevoir et dimensionner un Network Operations Center (NOC) et, si pertinent, un Security Operations Center (SOC) ;
 - Définir les processus ITSM/ITOM, les outillages de monitoring, les SLA internes et les exigences de maintenance préventive/corrective.
- 9. Besoins en équipements et infrastructures
 - Établir la nomenclature détaillée (routeurs, commutateurs, fibres, antennes, racks, onduleurs, climatisation, outils de gestion, licences, les besoins en énergie pour chaque site etc.) et chiffrer le CAPEX/OPEX.
- 10. Modèle de gouvernance et cadre réglementaire
 - Proposer le modèle institutionnel (rôles, responsabilités, financement, partages de coûts), les ajustements légaux et les politiques de sécurité/opération.
- 11. Plan de déploiement évolutif et de priorisation
 - Définir une roadmap par phases : sites prioritaires, provinces pilotes, services critiques ;
 - Articuler jalons, interdépendances, quick wins et critères de passage à l'échelle.
- 12. Plan de gestion du changement et de renforcement des capacités
 - Prévoir la formation, l'accompagnement des utilisateurs et des équipes techniques, ainsi que la transition opérationnelle (knowledge transfer).
- 13. Élaboration des Dossiers d'Appels d'Offres (DAO)
 - Rédiger les DAO et les spécifications techniques pour chaque lot (infrastructure, services, NOC, maintenance), intégrant critères d'évaluation et clauses de performance.

3. PORTÉE DE L'ÉTUDE / ACTIVITÉS À RÉALISER

La mission du cabinet consistera à :

1. **Cartographier les infrastructures existantes** : fibre optique, liaisons radio, VSAT, 4G/5G, data centers, équipements actifs, salles serveurs, capacité fibre optique utilisable par le gouvernement conformément à l'arrêté interministériel. Identifier les contraintes particulières des zones à haut risque ou difficilement accessibles (Ituri, Nord-Kivu, Sud-Kivu, Tanganyika, Haut-Uélé, Bas-Uélé, etc.).
2. **Analyser les besoins fonctionnels et techniques** des administrations (connectivité, stockage, QoS, cybersécurité, etc.).
3. **Élaborer des scénarios d'architecture réseau** : fibre, liaisons louées, satellite, etc., en analysant CAPEX/OPEX et risques, et **garantir l'interopérabilité technique et fonctionnelle des plateformes nationales existantes** ;
4. **Établir les règles de décision "déployer vs louer"** auprès des ISP ou autres partenaires.
5. **Dimensionner le réseau** (backbone, agrégation, LAN, NOC/SOC, services numériques, etc.). Définir des scénarios spécifiques de dimensionnement et de résilience pour les zones à haut risque
6. **Définir les services GovNet** : VPN, VoIP, messagerie sécurisée, cloud interne, supervision, etc.

7. **Concevoir un modèle de supervision et d'exploitation** (ITSM, SLA, NOC/SOC).
8. **Proposer un modèle de gouvernance** : rôles, responsabilités, cadre légal et institutionnel.
9. **Planifier un déploiement évolutif** : phasage, quick wins, priorités provinciales.
10. **Élaborer un plan de gestion du changement** et un programme de renforcement des capacités. Intégrer les zones à haut risque dans la stratégie de déploiement progressive en prévoyant des approches adaptées (satellite, radio, mutualisation d'infrastructures, déploiement différencié).
11. **Organisation de consultations formelles** avec les opérateurs publics et privés (SCPT, Liquid, Starlink, etc.).
12. Élaboration d'une stratégie spécifique pour les zones à haut risque intégrée à l'ensemble des scénarios de dimensionnement, de gouvernance et de déploiement du GovNet.
13. Production d'un modèle SIG géoréférencé (.shp/.geojson) des infrastructures recensées.
14. Développement d'une maquette technique interactive de l'architecture cible comprenant :
 - les schémas détaillés de l'architecture cible sous format Visio, Draw.io ou équivalent ;
 - les flux réseau principaux ;
 - les interactions entre GovNet, les centres de données, le Cloud Souverain et le GovSOC ;
 - une représentation fonctionnelle du NOC ;
 - les scénarios de montée en charge et de résilience.
15. **Rédiger les dossiers d'appels d'offres (DAO)** pour les différents lots d'infrastructure et services.
16. **Organisation et animation des ateliers de validation des livrables en coordination avec l'UGPTN.** Les ateliers minimums attendus sont :
 - Atelier de cadrage ;
 - Atelier de validation du diagnostic ;
 - Atelier de validation du schéma directeur et de l'étude de faisabilité ;
 - Atelier de validation des DAO ;
 - Atelier de restitution finale.

ACTIVITES A REALISER

ACTIVITÉ 1 – Cartographie et évaluation de l'existant

Objectif : établir une base de référence technique précise.

Tâches à réaliser :

- Recenser les infrastructures TIC existantes : fibre optique (publique/privée), faisceaux hertziens, VSAT, 4G/5G, réseaux radio.

- Identifier les équipements actifs (switches, routeurs), data centers, salles serveurs, installations locales.
- Évaluer l'état des LAN dans les bâtiments publics (administrations, ministères, hôpitaux, etc.).
- Localiser et caractériser les dispositifs de supervision en place (NOC, SOC).
- Mesurer les capacités actuelles et l'utilisation des ressources réseau : bande passante, taux de disponibilité, résilience, conformité aux normes (énergie, refroidissement, sécurité).
- Identifier les contraintes particulières des zones à haut risque ou difficilement accessibles (Ituri, Nord-Kivu, Sud-Kivu, Tanganyika, Haut-Uélé, Bas-Uélé, etc.).

ACTIVITÉ 2 – Analyse des besoins fonctionnels et techniques

Objectif : quantifier les exigences du réseau cible.

Tâches à réaliser :

- Identifier les besoins en connectivité des MDA (centrales, provinciales, locales).
- Évaluer les besoins en LAN, sécurité, stockage, PRA/PCA.
- Projeter les profils de trafic (actuels et futurs) selon différents scénarios d'usage (télétravail, e-services, etc.).
- Identifier les besoins en services (VoIP, messagerie, vidéoconférence, DNS, supervision, etc.).
- Établir les exigences de qualité de service (QoS) et de continuité d'activité.
- Identifier les corridors de fibre optique concernés par l'arrêté interministériel.
- Quantifier la capacité effectivement disponible pour l'État sur chaque corridor en termes de bande passante, fibres noires, longueurs et disponibilité.
- Évaluer les modalités techniques, juridiques et opérationnelles permettant l'activation de ces capacités.
- Identifier et cartographier les plateformes numériques gouvernementales existantes (e-Foncier, DGRAD, CNSSAP, e-Visa, Cloud Souverain, Guichet Unique, SNIP, etc.).
- Inventorier les mécanismes d'échange existants (API, Web Services, ESB, middleware, protocoles d'intégration).
- Évaluer la faisabilité technique de leur intégration au GovNet.

ACTIVITÉ 3 – Élaboration des scénarios d'architecture du réseau GovNet

Objectif : proposer plusieurs modèles technico-économiques.

Tâches à réaliser :

- Développer plusieurs scénarios de déploiement (backbone propriétaire, infrastructure partagée, location de fibre, mix satellite/fibre, etc.) qui prennent en compte la capacité fibre optique revenant de droit au gouvernement conformément à l'arrêté interministériel.
- Décrire pour chaque scénario : topologie, technologies utilisées, évolutivité, performances attendues.
- Chiffrer les CAPEX et OPEX.
- Analyser les avantages/inconvénients, les risques techniques et opérationnels.
- Formuler des hypothèses claires de croissance et d'usage.

ACTIVITÉ 4 – Règles de décision “déployer vs louer”

Objectif : orienter les décisions d'investissement du gouvernement.

Tâches à réaliser :

- Définir des critères objectifs pour le choix entre déploiement propriétaire et location auprès des FAI/infrastructure privée (distance, densité, coût, criticité).
- Proposer des modèles hybrides adaptés au contexte congolais.
- Évaluer les conditions contractuelles, les marges de négociation, les obligations de service minimum.

- Proposer les mécanismes d'exploitation de la capacité revenant à l'État, notamment les modèles d'IRU, conventions d'accès, SLA et accords opérationnels avec les opérateurs concernés.

ACTIVITÉ 5 – Dimensionnement détaillé du réseau

Objectif : produire un modèle technique chiffré et opérationnel.

Tâches à réaliser :

- Calculer les capacités nécessaires sur tous les segments : interprovincial, intra-ville, intra-bâtiment.
- Dimensionner les liens WAN, les LAN, les équipements d'agrégation et les connexions inter-DC.
- Préciser les niveaux de redondance et de résilience à chaque niveau.
- Estimer le volume de données à transporter selon les profils d'usage.
- Définir des scénarios spécifiques de dimensionnement et de résilience pour les zones à haut risque.

ACTIVITÉ 6 – Définition des services GovNet et des couches applicatives

Objectif : spécifier l'offre de services à rendre possible par le réseau.

Tâches à réaliser :

- Définir les services GovNet : VPN multisite, VoIP, PKI, DNS, e-mail sécurisé, supervision, authentification, etc.
- Proposer des architectures logicielles pour les services partagés.
- Assurer leur compatibilité avec l'interopérabilité et la souveraineté numérique.
- Définir les exigences d'interopérabilité réseau et applicative nécessaires à l'intégration des plateformes gouvernementales existantes et futures.

ACTIVITÉ 7 – Conception du modèle de supervision, maintenance et exploitation

Objectif : assurer la pérennité technique du GovNet.

Tâches à réaliser :

- Concevoir l'architecture et les fonctions du NOC et évaluer les interfaces nécessaires avec le GovSOC en cours de mise en œuvre. Lorsque pertinent, proposer les capacités complémentaires devant être intégrées au GovSOC ou prises en charge directement par GovNet.
- Définir les processus ITSM / ITOM (incident, changement, performance, etc.).
- Identifier les outils de monitoring, d'inventaire, de gestion de configuration.
- Fixer les niveaux de service internes (SLA) et les exigences de maintenance.

ACTIVITÉ 8 – Élaboration de la nomenclature technique et du chiffrage CAPEX/OPEX

Objectif : estimer les coûts totaux.

Tâches à réaliser :

- Dresser une nomenclature détaillée des équipements à acquérir (actifs, passifs, énergie, climatisation, logiciels, etc.).
- Établir les quantités, marques/références indicatives, coûts unitaires.
- Évaluer le coût de fonctionnement sur 5 à 10 ans (maintenance, licences, énergie, etc.).
- Identifier les postes budgétaires critiques.

ACTIVITÉ 9 – Définition du modèle de gouvernance et cadre réglementaire

Objectif : garantir la clarté institutionnelle et la soutenabilité du projet.

Tâches à réaliser :

- Proposer un modèle institutionnel (rôles, responsabilités, schémas de redevabilité).
- Identifier les ajustements nécessaires du cadre juridique ou réglementaire.
- Proposer des politiques de sécurité et de gestion opérationnelle du réseau.

- Étudier les modèles de partage des coûts (entre administrations, niveaux de gouvernement, etc.).

ACTIVITÉ 10 – Plan de déploiement évolutif et priorisation

Objectif : structurer une stratégie pragmatique et progressive.

Tâches à réaliser :

- Identifier les sites prioritaires (impact, maturité, disponibilité d'infrastructures).
- Définir une feuille de route par phase : pilotes, montée en charge, généralisation.
- Détailler les jalons clés, les quick wins, les interdépendances.
- Anticiper les ressources requises à chaque phase.
- Intégrer les zones à haut risque dans la stratégie de déploiement progressive en prévoyant des approches adaptées (satellite, radio, mutualisation d'infrastructures, déploiement différencié).

ACTIVITÉ 11 – Gestion du changement et renforcement des capacités

Objectif : assurer l'appropriation du réseau et sa durabilité.

Tâches à réaliser :

- Identifier les besoins de nouvelles ressources et de formation des techniciens, décideurs, administrateurs réseaux.
- Proposer un plan de formation structuré (contenus, modalités, calendrier).
- Prévoir les activités de sensibilisation et de transfert de compétences.
- Intégrer les mesures d'accompagnement au changement dans la stratégie globale.

ACTIVITÉ 12 – Élaboration des Dossiers d'Appel d'Offres (DAO)

Objectif : préparer la phase de mise en œuvre.

Tâches à réaliser :

- Rédiger les DAO par lot (réseaux, services, équipements, supervision).
- Définir les spécifications techniques, critères d'évaluation, exigences de performance.
- S'assurer que les DAO soient conformes aux normes de passation des marchés de la Banque mondiale et de la RDC.
- Préparer les annexes, formulaires, grilles de notation et canevas contractuels.
- Élaboration d'une stratégie spécifique pour les zones à haut risque intégrée à l'ensemble des scénarios de dimensionnement, de gouvernance et de déploiement du GovNet.

4. RESULTAT ATTENDUS

À l'issue de la mission, les résultats suivants sont attendus :

- Diagnostic complet de l'existant (infrastructures et capacités actuelles).
- Scénarios d'architecture technico-économiques documentés.
- Note de validation des hypothèses technico-économiques.
- Modèle optimal de déploiement du GovNet national, intégrant l'interopérabilité et les contraintes énergétiques.
- Dimensionnement technique détaillé (backbone, LAN, NOC, SOC).
- Nomenclature complète des équipements nécessaires.
- Modèle de gouvernance clair et soutenu par un cadre réglementaire.

- Plan de déploiement phasé, avec calendrier et priorités géographiques et mesures spécifiques pour les zones sensibles.
- Plan de formation et stratégie de changement institutionnel.
- DAO prêts à publication pour chaque lot identifié.
- Maquette technique ou démonstrateur numérique de l'architecture cible.

5. LIVRABLES ATTENDUS

1. Une note de cadrage redéfinissant et situant la mission
2. Le document stratégique du Schéma directeur et l'étude de faisabilité :
 - a. Rapport de diagnostic de l'existant (infrastructures et besoins).
 - b. Document de scénarios d'architecture et analyse comparative CAPEX/OPEX.
 - c. Rapport de dimensionnement technique du réseau.
 - d. Modèle de gouvernance et de cadre institutionnel proposé.
 - e. Plan de déploiement chiffré progressif et phasé.
3. Programme de renforcement des capacités et gestion des changements
4. Dossiers d'Appels d'Offres (DAO) complets (spécifications, critères, clauses).
5. Présentations de restitution aux parties prenantes.
6. Rapport final consolidé.

No	Livrables et détails	Durée	Jalon de validation	Pourcentage de paiement
1	Une note de cadrage redéfinissant et situant la mission	1 mois après la signature du contrat	Atelier de cadrage	10%
2	Rapport de diagnostic + modèle SIG géoréférencé	2.5 mois après la signature du contrat	Atelier diagnostic	15%
3	Schéma directeur et l'étude de faisabilité (évolutive) + note de validation des hypothèses	4.5 mois après la signature du contrat	Atelier stratégique	20%
4	Le plan de renforcement de capacités et gestion des changements	6 mois après la signature du contrat	Atelier capacités	15%
5	Maquette technique interactive de l'architecture cible (Visio/Draw.io ou équivalent) accompagnée des DAO complets.	7.5 mois après la signature du contrat	Atelier DAO	20%
6	Rapport de fin de mission consolidé	9 mois après la signature du contrat	Atelier de clôture	20%

6. PROFIL DU CABINET ET PERSONNEL CLE

Le cabinet devra répondre aux critères suivants :

- Expérience avérée dans **l'ingénierie et le déploiement de réseaux gouvernementaux**.
- Expertise en **dimensionnement et conception de réseaux IP/MPLS, SD-WAN, 5G, fibre optique, etc.**
- Expérience en **études de faisabilité technico-économiques et en architecture des infrastructures de télécommunication**.
- Références solides dans la **réalisation d'études similaires en Afrique ou dans des pays en développement**.
- Maîtrise des **normes et standards internationaux (ITU, ISO, IEEE, etc.)** pour les réseaux gouvernementaux.

Profil recherché :

- Cabinet ou consortium ayant une expertise démontrée en architecture réseau, dimensionnement d'infrastructure TIC, et déploiement de réseaux gouvernementaux ou critiques.
- Expérience dans au moins 3 projets similaires dans des contextes équivalents (gouvernements, projets à échelle nationale, pays en développement), et présenter au moins une référence pertinente de mission antérieure de mise en place de NOC..
- Maîtrise des standards internationaux en matière de réseaux sécurisés, d'architecture GovNet, de cybersécurité et de supervision.

Équipe clé attendue :

- **Chef de mission – Ingénieur télécom senior** avec au moins 10 ans d'expérience sur des projets similaires.
- **Expert en architecture réseau** (backbone/LAN/WAN, QoS).
- **Expert en cybersécurité et gouvernance IT** (avec certifications CISSP, CISM ou équivalent).
- **Spécialiste en supervision/NOC/SOC**.
- **Expert en passation des marchés publics ou DAO**.
- **Expert financier/économiste TIC** (analyse CAPEX/OPEX).

La pondération des Critères de qualification de la DP sont les suivants :

- Pertinence et qualité de l'expérience antérieure (10 points)
- Compréhension de la mission et méthodologie (25 points)
- Qualification de l'équipe proposée (55 points)
- Transférabilité des compétences et renforcement de capacités locales (5 points)
- Présence ou capacité de déploiement en RDC (5 points)

Personnel clé requis :

- **Chef de projet** : Expert en gestion de projets TIC et infrastructures réseau.
- **Architecte réseau** : Spécialiste en conception et dimensionnement de réseaux IP/MPLS et SD-WAN.
- **Ingénieur en télécommunications** : Spécialiste en fibre optique, micro-ondes, Satellite, VSAT et 5G.
- **Expert en cybersécurité** : Garant de la sécurité des communications et des infrastructures.
- **Spécialiste en modèles économiques et financement des infrastructures numériques.**
- **Expert en Services TIC utilisés au sein du Gouvernement**
- **Spécialiste en supervision / NOC / SOC**

Chef de Projet - Expert en gestion de projets TIC et infrastructures réseau

Formation :

- Bac+5 en télécommunications, informatique, réseaux ou ingénierie
- Certifié PMP, PRINCE2 ou équivalent (atout)

Expérience :

- Minimum 10 ans dans la gestion de projets TIC ou télécom
- Expérience avérée dans le pilotage de projets de réseaux gouvernementaux ou nationaux
- Maîtrise des enjeux institutionnels et de la coordination multi-acteurs

Compétences clés :

- Management d'équipes pluridisciplinaires
- Suivi budgétaire et reporting
- Bonne connaissance des réglementations télécoms et infrastructures numériques en Afrique

Architecte Réseau - Spécialiste en conception et dimensionnement IP/MPLS et SD-WAN

Formation :

- Bac+5 en ingénierie télécoms, réseaux ou équivalent
- Certifications recommandées : Cisco CCNP/CCIE, Juniper JNCIP ou toute certification professionnelle équivalente reconnue dans le domaine des architectures réseaux IP/MPLS, SD-WAN et infrastructures critiques.

Expérience :

- Minimum 8 ans en design et dimensionnement de réseaux IP/MPLS
- Maîtrise des architectures de backbone, réseaux sécurisés et infrastructures critiques
- Expérience de projets en Afrique ou dans des pays en développement

Compétences clés :

- Design de topologies réseau résilientes
- Dimensionnement en QoS, SLA
- Maîtrise des protocoles BGP, OSPF, MPLS, VPN, SD-WAN

Ingénieur Télécom - Spécialiste fibre optique, micro-ondes, VSAT et 5G

Formation :

- Bac+5 en télécommunications ou génie électrique
- Certifications techniques appréciées

Expérience :

- Minimum 8 ans sur le terrain (réseaux fibre optique, liaisons micro-ondes, VSAT)
- Expérience en dimensionnement et déploiement de réseaux dans des zones complexes ou rurales
- Connaissance des standards ITU et meilleures pratiques d'ingénierie réseau

Compétences clés :

- Planification et relevés terrain
- Études de faisabilité technologique
- Conception de liaisons fibre et radio

Expert en Cybersécurité - Sécurité des communications et infrastructures**Formation :**

- Bac+5 en cybersécurité, télécoms ou informatique
- Certifications: ISO 27001 Lead Implementer, CISSP, CISM, CEH (atouts)

Expérience :

- Minimum 8 ans en sécurité des systèmes critiques et réseaux
- Connaissance des normes ISO/IEC 27001, NIST, GDPR
- Expérience de sécurisation d'infrastructures e-Gov ou nationales

Compétences clés :

- Audit de sécurité des infrastructures réseau
- Mise en place d'architectures sécurisées
- Politique de gestion des accès et des identités (IAM)

Spécialiste en Modèles Économiques et Financement des Infrastructures Numériques**Formation :**

- Bac+5 en économie, finance, ingénierie économique ou management des infrastructures

Expérience :

- Minimum 8 ans dans la modélisation financière de projets d'infrastructures numériques
- Expertise dans l'élaboration de business models et de stratégies de financement (PPP, financement mixte, etc.)
- Expérience avec des bailleurs comme la Banque Mondiale, l'AFD ou l'UE

Compétences clés :

- Estimation CAPEX/OPEX
- Scénarios de financement et durabilité
- Analyse coûts-avantages

Expert en Services TIC utilisés au sein du Gouvernement**Formation :**

- Bac+5 en systèmes d'information, administration publique numérique, ingénierie informatique ou disciplines similaires.

Expérience :

- Minimum **8 ans d'expérience** dans l'analyse, la conception ou la gestion de **services TIC gouvernementaux** (e-gouvernement, téléservices, ERP publics, messagerie institutionnelle, vidéoconférence, plateformes numériques partagées, etc.).
- Expérience confirmée dans la **modélisation des besoins numériques des administrations publiques**, y compris dans les contextes africains ou à revenus intermédiaires.
- Connaissance des bonnes pratiques d'intégration des services TIC dans les architectures gouvernementales (interopérabilité, sécurité, résilience).

Compétences clés :

- Capacité à définir des **couches de services** à intégrer dans un intranet gouvernemental (VoIP, VPN, messagerie, services cloud, supervision, etc.).

- Maîtrise des référentiels ITIL, TOGAF, ou cadres comparables de gestion des services numériques.
- Connaissance des standards internationaux en matière de **services numériques publics** (ex. : Digital Public Infrastructure, Government Enterprise Architecture).
- Aptitude à collaborer avec les directions informatiques ministérielles, les agences e-gov, et les opérateurs TIC publics.

Rôle dans la mission :

- Identifier les services numériques essentiels à intégrer dans le GovNet (voix, données, sécurité, interopérabilité).
- Contribuer au **dimensionnement fonctionnel** et aux spécifications des services partagés.
- Appuyer la rédaction des **DAO relatifs aux couches applicatives** du GovNet.
- Veiller à l'alignement des services proposés avec les réalités opérationnelles des administrations congolaises.

Spécialiste en supervision / NOC / SOC

Formation :

- Bac+5 en télécommunications, systèmes informatiques, cybersécurité, ingénierie réseau ou discipline équivalente.

Expérience :

- Minimum **8 ans d'expérience** dans la conception, l'implémentation ou l'exploitation de **centres de supervision réseau (NOC)** et/ou de **centres de sécurité opérationnelle (SOC)**.
- Participation à au moins **deux projets similaires** de mise en place de centres NOC/SOC à l'échelle nationale, régionale ou pour des infrastructures critiques (gouvernements, opérateurs télécoms, infrastructures IT stratégiques).
- Connaissance approfondie des architectures de surveillance réseau, de gestion des événements de sécurité (SIEM), de détection des menaces et de réponse aux incidents.

Compétences clés :

- Maîtrise d'outils de supervision réseau et de cybersécurité reconnus sur le marché (ex. Nagios, Zabbix, SolarWinds ou équivalent ; Splunk, QRadar, AlienVault ou équivalent).
- Expérience en élaboration de procédures ITSM/ITOM : gestion des incidents, des problèmes, des changements, des SLA.
- Connaissance des normes et cadres de référence : ISO 27001, ISO 20000, NIST, COBIT, etc.
- Compétences en gestion d'équipe technique de supervision et exploitation.

Rôle dans la mission :

- Concevoir l'architecture cible du NOC et, si nécessaire, du SOC pour le réseau GovNet.
- Définir les outils, les équipements et les logiciels nécessaires à la supervision proactive et à la sécurité du réseau.
- Élaborer les **processus d'exploitation (SOP)**, les niveaux de service internes (SLA), les plans de continuité et de réponse aux incidents.
- Contribuer à la **formation du personnel local** chargé de l'exploitation et de la sécurité du réseau.

Autre Personnel

1. Expert SIG et Cartographie

Rôle :

- Réaliser la **cartographie des infrastructures existantes** (réseaux fibre, tours, stations VSAT...)
- Identifier les corridors technologiques optimaux
- Aider au dimensionnement en tenant compte du relief, des distances et de la géographie

Profil :

- Bac+5 en géomatique, génie civil ou télécoms
- Maîtrise des outils SIG (ArcGIS, QGIS)
- Expérience en projets TIC ou infrastructures linéaires

2. Juriste Spécialiste Régulation Télécom / Numérique**Rôle :**

- Analyser les **contraintes réglementaires et institutionnelles**
- Identifier les besoins en **cadre légal pour la gouvernance du réseau**
- Proposer des ajustements aux lois existantes (partage d'infrastructures, cybersécurité)

Profil :

- Juriste TIC, Bac+5 en droit du numérique
- Expertise en régulation télécoms, droit des infrastructures critiques
- Expérience en environnement africain

3. Expert en Énergie / Alimentation des Réseaux**Rôle :**

- Dimensionner les besoins énergétiques du réseau (Nœuds, Data centers)
- Proposer des solutions d'énergie solaire / hybride pour les sites isolés
- Réduire l'OPEX lié à l'énergie

Profil :

- Bac+5 en ingénierie électrique ou énergie
- Expérience en projets TIC avec contraintes énergétiques
- Maîtrise des solutions off-grid / hybridation

4. Expert Data Center & Cloud Infrastructure**Rôle :**

- Analyser la capacité d'hébergement nationale existante
- Proposer une architecture complémentaire : **cloud souverain**, hébergement sécurisé
- Assurer la continuité de service et la résilience

Profil :

- Bac+5 en informatique / cloud
- Certifié AWS/Azure ou Data Center Infrastructure (Uptime Tier, TIA-942)
- Expérience en infrastructures critiques

5. Analyste Socio-économique / Enjeux d'Impact**Rôle :**

- Évaluer les impacts socio-économiques du GovNet (emplois, accès services publics)
- Identifier les **zones prioritaires d'impact**
- Contribuer au **modèle de rentabilité sociale**

Profil :

- Bac+5 en socio-économie, économie du numérique
- Expérience en projets e-Gov ou transformation numérique

7. METHODOLOGIE ET DELAIS

Le cabinet proposera une **méthodologie détaillée** pour la réalisation de l'étude, incluant :

- La collecte et l'analyse des données existantes.
- Les consultations avec les parties prenantes (ministères, opérateurs télécoms, agences gouvernementales, etc.).

- L'élaboration des scénarios techniques et financiers.
- La validation des propositions avec les autorités compétentes.

Le délai maximal pour la réalisation de l'étude est de **9 mois** à compter de la signature du contrat.

8. MODALITE DE SOUMISSION

Une firme sera sélectionnée suivant la méthode de Sélection Fondée sur la Qualité et le Coût (SFQC) conformément au Règlement de de Passation des Marchés pour les Emprunteurs sollicitant le financement des projets d'investissement la Banque mondiale, édition de septembre 2025.

