RÉPUBLIQUE DU TCHAD
****
PRÉSIDENCE DE LA RÉPUBLIQUE
****
PRIMATURE
****
MINISTÈRE DES TÉLÉCOMMUNICATIONS, DE L'ÉCONOMIE NUMÉRIQUE ET DE LA DIGITALISATION DE L'ADMINISTRATION
****
SECRÉTARIAT GÉNÉRAL
****
PROJET D'APPUI À LA TRANSFORMATION NUMÉRIQUE DU TCHAD (PATN)

LA BANQUE MONDIALE
BIRD • IDA | GROUPE DE LA BANQUE MONDIALE

PATN
Projet d'Appui à la Transformation Numérique du Tchad

TERMES DE RÉFÉRENCE (TDR)

ANSICE	ÉLABORATION DE LA POLITIQUE NATIONALE DE CYBERSÉCURITÉ (PNC) DU TCHAD

1 Contexte et Justification

Le Tchad connaît une transformation numérique rapide, portée par des initiatives stratégiques telles que *Tchad Connexion 2030*, visant à moderniser les infrastructures numériques et à promouvoir les services en ligne. Cependant, cette évolution s'accompagne d'une augmentation des cybermenaces : attaques ciblant les systèmes d'information critiques, cybercriminalité organisée, fuites de données, etc.

En 2023, le pays a adopté sa première Stratégie Nationale de Cybersécurité (SNC), définissant les orientations générales en matière de sécurité numérique. La mise en œuvre effective de cette stratégie nécessite un **Plan National de Cybersécurité (PNC)** détaillé, opérationnel et assorti d'indicateurs de performance.

Ce plan devra :

- Traduire la stratégie en actions concrètes, chiffrées et planifiées.
- Définir clairement les rôles des parties prenantes.
- Intégrer les standards et bonnes pratiques internationales (ISO/IEC 27001, NIST, Convention de Budapest).

Le Ministère des Télécommunications, de l'Économie Numérique et de la Digitalisation de l'Administration, à travers le Projet d'Appui à la Transformation Numérique du Tchad (PATN), souhaite recruter un cabinet spécialisé pour élaborer ce plan.

2 Objectifs de la Mission

2.1 Objectif général

Mettre en place un Plan National de Cybersécurité complet, réaliste et opérationnel, permettant de renforcer la résilience numérique du Tchad et d'assurer la protection de ses systèmes d'information critiques.

2.2 Objectifs spécifiques

Le cabinet devra :

1. Évaluer l'état actuel des capacités nationales en cybersécurité (diagnostic technique, organisationnel et réglementaire).
2. Identifier et prioriser les actions nécessaires à court, moyen et long terme.
3. Définir une gouvernance claire pour la mise en œuvre du plan.
4. Proposer un cadre réglementaire et institutionnel adapté.
5. Intégrer un programme de sensibilisation, de formation et de développement des compétences.
6. Élaborer un plan de suivi-évaluation avec indicateurs.

3 Portée de la Mission

Le cabinet sera chargé de :

3.1 Diagnostic et analyse

- Collecte et analyse des données sur l'état des infrastructures critiques, la législation en vigueur et les capacités institutionnelles.
- Benchmark avec d'autres pays africains et standards internationaux.

3.2 Élaboration du plan

- Définition des axes stratégiques et actions prioritaires.
- Planification budgétaire et calendrier de mise en œuvre.
- Identification des sources de financement potentielles (nationales et internationales).

3.3 Gouvernance et cadre réglementaire

- Proposition d'un schéma institutionnel clair.
- Recommandations pour la mise à jour ou l'adoption de textes législatifs et réglementaires.

3.4 Sensibilisation et renforcement des capacités

- Élaboration d'un programme de formation et de sensibilisation.
- Intégration de la cybersécurité dans les cursus éducatifs et la formation continue.

3.5 Suivi et évaluation

- Conception d'un mécanisme de suivi-évaluation.
- Définition d'indicateurs de performance.

4 Résultats attendus

1. Rapport de diagnostic national en cybersécurité.
2. Plan National de Cybersécurité validé.
3. Cadre institutionnel et réglementaire proposé.
4. Plan de formation et de sensibilisation.
5. Guide de mise en œuvre avec indicateurs de suivi.

5 Profil du Cabinet et des Experts Requis

5.1 Expérience Générale du Cabinet

- Être un cabinet international spécialisé en cybersécurité, reconnu pour son expertise dans l'élaboration et la mise en œuvre de politiques, stratégies et plans nationaux de cybersécurité.
- Justifier d'au minimum 10 années d'expérience avérée dans le domaine, couvrant la gouvernance cyber, le renforcement des capacités, l'élaboration de cadres réglementaires, ainsi que la mise en place de dispositifs techniques et organisationnels de sécurité.
- Avoir conduit avec succès des missions similaires dans au moins deux pays au cours des cinq (5) dernières années, avec livrables validés au niveau national et, idéalement, financés par des partenaires techniques et financiers internationaux.
- Disposer d'une expérience avérée en Afrique, avec une bonne connaissance des environnements réglementaires, institutionnels et opérationnels des pays en développement ; l'expérience en zone CEMAC constituera un atout majeur.

- Démontrer sa capacité à travailler dans des environnements multiculturels et multilingues, en mobilisant à la fois des experts internationaux et locaux.
- Présenter des références vérifiables incluant la description des missions, les résultats obtenus, les bénéficiaires, les budgets et les contacts des donneurs d'ordre pour vérification.
- Justifier d'une expérience de coordination multisectorielle (gouvernement, secteur privé, société civile, milieux académiques) dans le cadre de projets de cybersécurité à l'échelle nationale ou régionale.

5.2 Profil des experts clés

Poste	Qualification	Expérience minimale	Certifications recommandées	Effort (H/M)
Chef de mission – Expert en cybersécurité stratégique	Bac+5 en sécurité informatique, télécoms ou domaine connexe	15 ans en stratégie et gouvernance cyber	CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional) ou équivalent	5
Expert en cadre légal et réglementaire	Bac+5 en droit du numérique ou équivalent	10 ans en réglementation cyber et protection des données	Certification en protection des données (ex. : CIPP/E – Certified Information Privacy Professional/Europe) ou équivalent	3
Expert technique en sécurité des SI	Bac+5 en sécurité informatique ou réseaux	10 ans en audit et protection des SI	ISO/IEC 27001 Lead Auditor ou Lead Implementer, CEH (Certified Ethical Hacker) ou équivalent	4
Expert en sensibilisation et formation cyber	Bac+5 en ingénierie pédagogique	8 ans en formation et culture cyber	Certification en pédagogie ou en sensibilisation sécurité (ex. : CompTIA Security+ ou équivalent)	2

NB : L'équipe proposée à ce stade ne fait pas l'objet d'une évaluation. Toutefois, des profils minimums devront être décrits pour vérification de la capacité technique du soumissionnaire.

6 Durée et lieu de la mission

La mission durera **six (6) mois** et se déroulera entièrement à **N'Djaména**, avec des déplacements ponctuels chez les opérateurs et institutions pour collecter des données. Le cabinet devra prévoir un moyen de déplacement adapté.

Le cabinet devra prévoir un **moyen de déplacement adapté** (véhicule avec chauffeur ou solution équivalente) pour faciliter ces missions sur site.

Les principales phases de la mission sont les suivantes :

Phase	Durée estimative	Lieu	Principales activités	Livrables
1. Préparation et cadrage	3 semaines	N'Djaména Siège ANSICE	- Réunion de lancement avec l'ANSICE et parties prenantes - Validation de la méthodologie et du plan de travail détaillé - Revue documentaire et préparation des outils de collecte	- Plan de travail validé - Méthodologie approuvée - Outils de collecte opérationnels

2. Diagnostic national et analyse comparative	4 semaines	N'Djaména Sièges des parties prenantes	- Collecte et analyse des données techniques, organisationnelles et réglementaires - Entretiens avec les parties prenantes (public, privé, société civile, partenaires internationaux) - Évaluation de la maturité cybersécurité nationale - Benchmark régional et international	- Rapport de diagnostic - Cartographie des risques et maturité cyber - Rapport de benchmark
3. Conception du Plan National de Cybersécurité	6 semaines	N'Djaména	- Définition des axes stratégiques et actions prioritaires - Élaboration du cadre de gouvernance - Proposition du cadre réglementaire - Planification budgétaire et identification des financements	- Projet de PNC complet avec actions, budget et calendrier - Schéma de gouvernance proposé - Recommandations réglementaires
4. Validation et ajustements	3 semaines	N'Djaména – Ateliers multisectoriels	- Organisation d'ateliers de validation - Intégration des observations et ajustements - Validation finale par le Comité technique et autorités compétentes	- PNC validé - Compte rendu des ateliers
5. Formation et transfert de compétences	2 semaines (10 jours ouvrables, en 2 sessions de 5 jours)	N'Djaména – Salle équipée	**Objectif** : Assurer la pérennité du PNC par le renforcement des compétences des acteurs nationaux **Public cible** : Responsables cybersécurité des ministères, points focaux opérateurs, RSSI d'infrastructures critiques, forces de sécurité, secteur judiciaire **Modules** : **Module 1 : Gouvernance et gestion stratégique de la cybersécurité** • Cadre de gouvernance du PNC. • Coordination interinstitutionnelle et rôles des parties prenantes. **Module 2 : Cadre légal et réglementaire** • Législation nationale et obligations réglementaires. • Conformité aux standards internationaux (ISO/IEC 27001, RGPD, NIST). **Module 3 : Gestion opérationnelle de la cybersécurité** • Processus de prévention, détection, réponse et reprise après incident.	- Guides méthodologiques - Supports pédagogiques - Rapport de formation avec liste des participants et évaluation des acquis - Recommandations pour poursuite du renforcement de capacités

			• Gestion des vulnérabilités et mise à jour des mesures de sécurité. **Module 4 : Suivi-évaluation et indicateurs de performance** • Méthodes de collecte et analyse des indicateurs du PNC. • Élaboration des rapports de suivi et d'évaluation. **Module 5 : Sensibilisation et culture cybersécurité** • Techniques de communication pour promouvoir les bonnes pratiques. • Campagnes nationales de sensibilisation. **Méthodes** : Approche participative et interactive. Études de cas et exercices pratiques adaptés au contexte tchadien. Simulation d'incidents cyber (table-top exercice). Utilisation d'outils et plateformes de démonstration. **Modalités** : Évaluation des acquis en fin de formation	
6. Assistance technique post-livraison	4 semaines	N'Djaména ANSICE et institutions bénéficiaires	- Appui à la mise en œuvre initiale du PNC - Accompagnement dans la mise en place des premiers indicateurs de suivi - Conseil technique pour les premières actions opérationnelles	- Rapport d'assistance technique - Suivi de la mise en œuvre initiale - Tableau de bord des premiers indicateurs

7 Coordination et supervision

Le cabinet travaillera en étroite collaboration avec l'ANSICE, sous la supervision d'un **Comité de gestion du projet** chargé de :

- Valider les livrables.
- Suivre l'avancement de la mission.
- Superviser les ateliers de validation.

8 Lieu et Date de Soumission

Les cabinets intéressés sont invités à soumettre leur dossier sous pli fermé à l'adresse suivante :

À l'attention du Coordonnateur National de l'UGP-PATN au plus tard le 10 novembre 2025 le à 15 heures 30 minutes au bureau du Spécialiste en Passation des Marchés du Projet PATN, Sis au quartier Farcha dans le 1er Arrondissement, Avenue Nelson Mandela, Rue 1402 et Porte 1183 et collée à l'agence SAAR Assurances. Courriel : contact@patn.td Tel : (+235) 85 80 74 10 N'Djaména-Tchad. Tous les jours de 7 heures 30 minutes à 15 heures 30 minutes et le vendredi de 7 heures 30 minutes à 12 heures précises.

9 Méthode de sélection

Le Consultant sera sélectionné selon la méthode de **Sélection Fondée sur les qualifications des Consultants**, Conformément au Règlement de Passation des Marchés pour les Emprunteurs sollicitant le financement de Projets d'Investissement (FPI), Sixième Edition de Février 2025 et disponible sur le site de la Banque Mondiale : www.worldbank.org et conformément aux critères exigés au regard des présents termes de référence ».