BCRG
BANQUE CENTRALE DE LA RÉPUBLIQUE DE GUINÉE

Conakry, le 09 AVR. 2025

AVIS D'APPEL D'OFFRES

Dans le cadre de l'exécution de son programme budgétaire 2025, la Banque Centrale de la République de Guinée (BCRG) se propose de recruter un consultant dans le cadre de la mise en place d'un programme de cybersécurité.

A cet effet, elle lance le présent appel à concurrence et invite tous les cabinets spécialisés dans ce domaine à y répondre en soumettant leurs offres.

La consultation est ouverte à tous les cabinets agréés constitués sous forme de société ou non et justifiant d'au moins trois (3) ans d'expérience dans le domaine de l'accompagnement en cyber sécurité.

Les Termes de Référence peuvent être obtenus auprès de la Direction du Système d'Information de la BCRG située au 1er étage du Bâtiment principal et sur le site Web de la BCRG.

Les offres doivent être présentées en quatre **(4) exemplaires**, dont **un (1) original** et **trois (3) copies**, le tout rédigé en Français et mises dans une enveloppe anonyme et déposée au Secrétariat de la Direction du Système d'Information (BCRG, 1ème étage,) au plus tard le ...16 MAI 2025.....**avant 16 heures**, date limite de dépôt des offres.

Les soumissionnaires demeurent engagés par leurs offres jusqu'à quatre-vingt-dix (90) jours, à compter de la date limite de remise des offres.

Les offres seront ouvertes en séance publique le .....19 MAI 2025.....par la Commission de dépouillement de la Banque Centrale.

Les candidats doivent strictement se conformer aux TDR joints au dossier sous peine de voir leurs offres purement et simplement rejetées.

BCRG BANQUE CENTRALE DE LA RÉPUBLIQUE 16/04/25

LA BANQUE CENTRALE

12, boulevard du Commerce, 6e avenue de la République C/Kaloum - BP 692 - Conakry - République de Guinée
Tél : (+224) 664 67 77 77 - Fax : (+224) 669 08 88 88 - mail : secretariat.gouv@bcrg-guinee.org
www.bcrg-guinee.org

Banque centrale de la République de Guinée

Direction des Systèmes d'Informations

TERMES DE REFERENCE

Relatif au recrutement d'un cabinet de consultants pour la mise en œuvre d'un programme de cybersécurité en faveur de la Banque Centrale de la République de Guinée

Mars 2025

TABLE DES MATIERES

I. Présentation de la Banque centrale

La Banque Centrale de la République de Guinée, en abrégé « BCRG », régie par la Loi L/2017/017/AN du 08 juin 2017, abrogeant la Loi L/2016/064/AN du 09/11/2016, elle-même, modifiant la Loi L/2014/016/2014 du 02 juillet 2014 portant son statut, sise à Almamya au 12, Boulevard du Commerce, 6ème Avenue de la République, Commune de Kaloum, B.P : 692 Conakry, représentée à l'effet des présentes par Dr. Karamo KABA, Gouverneur ;

La Banque Centrale de la République de Guinée (BCRG) a été créée en 1960 avec, comme principales missions, d'assurer la stabilité des prix et de promouvoir un système financier viable pour une croissance durable en République de Guinée.

A. **Missions de la BCRG**

De façon pratique, en tant que Banque Centrale, la BCRG :

- Assure la politique monétaire et de change ;
- Assure la supervision des institutions financières ;
- Assure la stabilité financière (lutte contre le blanchiment de capitaux et le financement du terrorisme) ;
- Effectue les opérations bancaires ;
- Promeut les moyens de paiement ;
- Assure l'émission, la circulation et le retrait des billets de banque et monnaies métalliques ;
- Effectue des opérations sur matières précieuses et devises étrangères ;
- Opère sur les marchés financiers ;
- Effectue des opérations de crédit avec des banques opérant en République de Guinée ;
- Tient les comptes du Trésor Public, des Collectivités Territoriales, des établissements de crédit assujettis, des établissements de crédit étrangers, des institutions financières et autres intermédiaires agréés, des Banques Centrales étrangères, des gouvernements étrangers, des organismes financiers internationaux, ainsi que des membres du gouvernement et agents de la Banque Centrale ;
- Effectue des opérations au profit du Trésor Public : émission de certaines valeurs du Trésor, conservation des valeurs et titres ;
- Gère ses propres placements et investissements.

B. **Organisation de la BCRG**

Le siège de la BCRG est situé à Conakry, la capitale du pays.

Le réseau de la BCRG comprend sept agences :

Une agence principale à Conakry ;
Une agence à Kankan ;
Une agence à Kindia ;
Une agence à Labé ;
Une agence à Nzérékoré ;
Une agence à Boké ;
Une agence à Mamou ;
Une agence à Faranah.

II. CONTEXTE ET JUSTIFICATIONS :

La Banque Centrale de la République de Guinée (BCRG) est un acteur clé du système financier national. Face à l'évolution croissante des cybermenaces et à l'accroissement des exigences réglementaires en matière de cybersécurité, la BCRG souhaite renforcer la protection de ses systèmes d'information en mettant en place un Programme de Cybersécurité structuré et aligné aux meilleures pratiques internationales.

Afin d'assurer une approche cohérente, stratégique et durable, la BCRG cherche à recruter un cabinet de conseil en cybersécurité disposant d'une expertise avérée pour l'accompagner dans l'élaboration et la mise en œuvre progressive de son programme de cyber sécurité.

Le cabinet retenu devra intervenir à chaque phase clé du programme, notamment pour :

- Réaliser un diagnostic de la posture de cybersécurité actuelle.
- Définir une stratégie et une feuille de route pluriannuelle.
- Assister la BCRG dans la sélection des solutions technologiques et des prestataires.
- Renforcer la gouvernance, la conformité et la sensibilisation en cybersécurité.

III. OBJECTIFS GENERAUX ET SPECIFIQUES

1. Objectif Général

L'objectif principal se structure en deux phases:

Phase 1: Concevoir et structurer un Programme de Cybersécurité permettant à la BCRG de renforcer la résilience de ses systèmes d'information, en conformité avec les normes et cadres internationaux (ISO 27001, NIST CSF, PCI-DSS, COBIT, etc.).
Phase 2: Déployer le programme de cybersécurité à travers l'élaboration et le déploiement des processus de sécurisation du système d'information, la formalisation du corpus documentaire associé, la formation et la sensibilisation des collaborateurs de la BCRG, ainsi que l'accompagnement au déploiement des solutions techniques de sécurité retenus.

2. Portée des missions et Objectifs spécifiques

Le cabinet de conseil interviendra principalement à un niveau stratégique et organisationnel. Son rôle consistera à orienter et accompagner la BCRG à travers les phases et étapes ci-dessous.

La Phase 1 du projet consistera à :

- **Diagnostiquer et évaluer l'existant**
  - Évaluer l'état actuel de la cybersécurité au sein de la BCRG et identifier les risques.
  - Évaluer le niveau de conformité avec les réglementations relatives à la cybersécurité qu'elles soient locales, internationales ou sectorielles.
  - Effectuer une cartographie des actifs critiques de la BCRG (infrastructures, données, applications, etc.).
  - Réaliser une analyse des risques et de la maturité de la cybersécurité (ISO 27005, EBIOS RM, ISO 27001 ou NIST).

- Identifier les vulnérabilités et menaces pesant sur les systèmes et les processus bancaires à travers un test d'intrusion interne et externe.
- Élaborer un rapport d'évaluation avec des recommandations stratégiques.

- **Élaborer une stratégie et une feuille de route pluriannuelle adaptée aux enjeux et contraintes de la BCRG.**
  - Etablir une feuille de route sur 3 ans déclinant la stratégie de sécurité du système d'informations de la BCRG
  - La feuille de route devra prendre en compte les capacités budgétaires et en termes de ressources humaines de la BCRG
  - Les chantiers de la feuille de route devront être évaluées en termes de priorité, complexité, budget, charges projet et d'exploitation
- **Définir une gouvernance de la cybersécurité avec des rôles et responsabilités clairs**
  - Définir une stratégie cybersécurité alignée avec les objectifs métiers et les exigences réglementaires.
  - Mettre en place une gouvernance avec des rôles et responsabilités clairs.
  - Proposition d'un organigramme de cybersécurité et d'une structure de gestion de la sécurité, fondée sur le cycle PDCA (Plan-Do-Check-Act).
- **Appuyer la BCRG dans la sélection des solutions et des fournisseurs**
  - Analyse des besoins en solutions techniques de sécurité: SIEM, EDR/XDR, SOAR, MFA, PAM, IDS/IPS, WAF, DLP, NDR, chiffrement, analyse de malware, etc.
  - Analyse des besoins en solutions de sécurité : SIEM, SOC, MFA, PAM, IDS/IPS, WAF, DLP, XDR, chiffrement, etc.
  - Évaluation des solutions disponibles sur le marché et assistance à la prise de décision.
  - Rédaction des cahiers des charges et des appels d'offres en définissant les critères techniques et fonctionnels.
  - Sélection des fournisseurs : analyse des offres, organisation de démonstrations et recommandations finales.
  - Définition d'un plan de mise en œuvre : feuille de route détaillée pour un déploiement efficace des solutions retenues.
- **Renforcement des capacités et sensibilisation**
  - Évaluer le niveau de maturité cyber des collaborateurs de la BCRG
  - Élaborer un plan de formation portant sur les thématiques de cybersécurité à destination des équipes de la Direction des Systèmes d'Information.
  - Concevoir une stratégie de sensibilisation pour l'ensemble du personnel.
- **Proposer un plan de suivi et de pilotage du programme en élaborant des indicateurs de suivi et de reporting pour mesurer l'efficacité du programme.**

La phase 2 : consistera à mettre en œuvre de manière opérationnelle la feuille de route établie lors de la phase 1 :

- **Formaliser et déployer les processus de sécurisation du système d'information nécessaires à la mise en œuvre d'un SMSI (Système de Management de la Sécurité de l'Information) :**
    - Formaliser le corpus documentaire SSI
    - Former les parties prenantes à la prise en main des processus établis
- **Déployer le plan de formation** à destination des collaborateurs de la DSI
    - Former les collaborateurs de la DSI afin de mettre en adéquation leurs compétences avec les enjeux de sécurité du système d'information
    - Faire former par les éditeurs et fournisseurs de solutions techniques, les collaborateurs de la DSI, aux technologies et solutions qui seront déployées
- **Déployer la stratégie de sensibilisation des collaborateurs de la BCRG**
- **Accompagner le déploiement des solutions techniques de sécurité retenues**
    - Cadrer les projets d'intégration de solutions techniques
    - Participer au pilotage des projets d'intégration
    - Contrôler et évaluer l'atteinte des objectifs fixés pour chaque projet d'intégration d'une solution technique

IV. LIVRABLES ATTENDUS

1. Rapport d'évaluation de la cybersécurité (analyse des risques et test d'intrusion)
2. Stratégie et feuille de route pluriannuelle (plan détaillé avec jalons, priorités et chiffrage macro).
3. Modèle de gouvernance et d'organisation de la cybersécurité (incluant une analyse d'impact organisationnel)
4. Cahiers des charges et documents d'appels d'offres pour les solutions et services à acquérir.
5. Plan de formation pour les membres de la Direction des Systèmes d'Information
6. Stratégie de sensibilisation de l'ensemble des collaborateurs de la BCRG
7. Comitologie de pilotage du programme, indicateurs de suivi et de reporting
8. Corpus documentaire de sécurité, nécessaire pour répondre aux enjeux de conformité et de sécurité de la BCRG
9. Formation des collaborateurs selon le plan de formation établi
10. Sensibilisation des collaborateurs selon de stratégie de sensibilisation établie

V. PROFIL DU CABINET DE CONSULTANTS

Le cabinet de consultants devra répondre aux critères suivants :

1. Expérience et Références

- Justifier d'au moins 5 années d'expérience en cybersécurité, avec une expertise avérée dans la mise en œuvre de programmes de cybersécurité.
- Disposer de consultants certifiés (CISSP, CISM, CEH, OSCP, ISO 27001, ISO 22301)
- Avoir une expertise en SOC, SIEM, Threat Intelligence et audits de sécurité
- Avoir une expérience dans la formation et la sensibilisation à la cybersécurité
- Disposer d'une expérience démontrée dans les standards internationaux de cybersécurité, notamment ISO 27001, NIST, PCI-DSS, COBIT, ITIL et autres cadres réglementaires appliqués aux institutions financières.

- Avoir réalisé au moins un projet similaire au cours des cinq dernières années (2020 - 2024), attesté par des lettres de bonne exécution.

2. Capacité Technique

- Avoir une expertise démontrée dans les technologies et méthodologies de cybersécurité, notamment :
    - Gouvernance de la cybersécurité et gestion des risques (ISO 27005, EBIOS).
    - Déploiement de solutions de protection des infrastructures IT (IDS/IPS, WAF, DLP, MFA, PAM, chiffrement).
    - Détection et réponse aux incidents (SIEM, SOC, Threat Intelligence, XDR, NDR).
    - Planification et exécution de tests de pénétration et audits de sécurité.
    - Élaboration de politiques et procédures de cybersécurité.
- Disposer d'un agrément des fabricants des équipements ou logiciels de cybersécurité proposés.

3. Équipe Projet et Certifications

Le cabinet devra mobiliser une équipe qualifiée, incluant à minima les profils suivants

3.1. Expert Chef d'Équipe

- Diplôme de niveau Bac+5 en Informatique, Télécommunications, Cybersécurité ou équivalent.
- Minimum 10 ans d'expérience en cybersécurité.
- Certifications recommandées : CISSP, PMP (Project Management Professional), PRINCE2 Practitioner ou CISM (Certified Information Security Manager).
- Compétences en gestion de projets complexes en cybersécurité, coordination d'équipes pluridisciplinaires, suivi des délais, budgets et livrables.
- Connaissance approfondie des normes et bonnes pratiques en cybersécurité (ISO 27001, NIST, CIS, etc.)
- Expérience démontrée dans au moins un projet similaire au cours des cinq dernières années.

3.2. Analystes Cybersécurité

- Diplôme Bac+5 en Informatique ou diplôme d'Ingénieur.
- Minimum 5 ans d'expérience en cybersécurité.
- Expérience en détection et gestion des incidents de cybersécurité.
- Certifications requises :
    - CEH – Certified Ethical Hacker (Obligatoire)
    - ISC2 Cybersecurity (Obligatoire)
    - ECIH - Certified Incident Handler (récommmandé)
- Justifier d'au moins un projet similaire réalisé et attesté par une lettre de bonne exécution.

3.3. Consultants Senior (Expert GRC) spécialiste en analyses de risques et en formation cybersécurité

- Minimum 10 ans dans la gestion des risques, la conformité et la gouvernance en cybersécurité.
- Expertise en analyses de risques (ISO 27005, EBIOS, etc.).
- Compétences en conception et animation de formations en cybersécurité.

- Maîtrise des normes et cadres de référence (ISO 27001, NIST CSF, RGPD).
- Certifications recommandées : ISO 27001 Lead Implementer ou Lead Auditor, ISO 27005

3.4 Consultants Senior Experts techniques (architectures sécurisés et intégration de solutions techniques)

- Minimum 10 ans en conception et déploiement d'architectures sécurisées et en intégration de solutions techniques.
- Conception d'architectures sécurisées (réseaux, cloud, systèmes).
- Intégration de solutions techniques (pare-feu, IAM, chiffrement, etc.).
- Expertise en sécurisation des environnements IT.

VI. Procédure de sélection

La soumission doit être rédigée en langue française et comporter les documents attestant de la régularité de sa situation vis-à-vis des organismes sociaux (sécurité sociale) et organismes ou autorité de tutelle.

Le soumissionnaire fournira dans trois (03) enveloppes séparées :

- offre technique,
- une offre financière, et ;
- un avant-projet de contrat.

Les trois (03) enveloppes seront insérées dans une (01) grande enveloppe portant les mentions suivantes :

« Appel à concurrence pour le recrutement d'un cabinet de consultants pour la mise en œuvre d'un programme de cyber sécurité à la Banque Centrale de la République de Guinée.

A Monsieur le Directeur des Systèmes d'Information de la BCRG

Boite Postale N° : 692, Conakry – République de Guinée.

1. Validité des offres

Le soumissionnaire reste engagé par son offre pendant une durée de quatre-vingt-dix (90) jours.

2. Réception des offres

Les offres doivent être déposées au secrétariat de la Direction des Systèmes d'Information, situé au 1er étage du bâtiment principal, Porte N 182.

La date limite de réception des offres est fixée au 16 MAI 2025

Toute offre parvenue après la date et l'heure limite indiquée ci-dessus sera considérée comme irrecevable.

3. Modalités de sélection

La grille de notation qui sera appliquée pour évaluer les offres est la suivante :

N°	Offre technique	Notes/ 70	Score
1	Note portant compréhension de la mission	20	
2	Méthodologie proposée	20	
3	Références et réalisations passées du cabinet	15	
	Qualifications et expériences de l'équipe projet	10	
4	Délai de mise en œuvre	5	
5	Total	70	

Offre Financière : 30

Total :100

L'examen des offres financières est conditionné par l'obtention d'une note minimale de 60/70 pour l'offre technique.

Le marché sera attribué au soumissionnaire qui présente le meilleur rapport qualité/prix.

La BCRG se réserve également la possibilité de ne donner suite à aucune des propositions présentées lorsque celles-ci s'écartent des besoins exprimés dans les présents TDR.

Conakry, le 16 AVR 2025

La Banque Centrale