SONAP
Société Nationale des Pétroles

REPUBLIQUE DE GUINEE

.....

Travail-Justice-Solidarité

PRESIDENCE DE LA REPUBLIQUE

SOCIETE NATIONALE DES PETROLES (SONAP)S.A

N°...../PRG/SONAP/DG/PRMP/2026

Avis d'Appel à Manifestation d'Intérêt

Intitulé sommaire des Prestations

1 - Le présent Avis à manifestation d'intérêt fait suite à la volonté de la Société Nationale des Pétroles (SONAP S.A) d'envisager la réalisation d'un audit global de sécurité de son système d'Information.

2 – La SOCIETE NATIONALE DES PETROLES (SONAP S.A) a obtenu dans le cadre de l'exécution de son budget des fonds. Et a l'intention d'utiliser une partie de ces fonds pour effectuer des paiements au titre du marché relatif à la réalisation d'un audit global de sécurité de son Système d'Information.

Le financement est à 100% assuré par le Budget de la Société Nationale des Pétroles (SONAP) SA.

3- Contexte et justification

a. Contexte

La Société Nationale des Pétroles de Guinée (SONAP) est un acteur stratégique du secteur des hydrocarbures en République de Guinée. Ses activités couvrent l'importation, le stockage, la distribution et la gestion des ressources pétrolières.

Le Système d'Information (SI) de la SONAP constitue un pilier essentiel de ses opérations.

Avec l'évolution croissante des cybermenaces et les risques spécifiques au secteur énergétique, la SONAP se doit de garantir un niveau élevé de sécurité de son SI afin d'assurer :

- La disponibilité et l'intégrité des infrastructures informatiques.
- La confidentialité des données, stratégiques et réglementaires.
- La résilience face aux cyberattaques et incidents de sécurité.

C'est dans ce cadre que la SONAP envisage la réalisation d'un audit global de sécurité de son Système d'Information.

b. Justification

L'audit vise à :

- Identifier et évaluer les vulnérabilités et les menaces pesant sur le Système d'Information.
- Apprécier le niveau de maturité de la gouvernance et des dispositifs de cybersécurité ;
- Vérifier la conformité aux normes et réglementations applicables (ISO 27001, ISO 27005, NIST, RGPD, Loi guinéenne sur la cybersécurité, etc.).
- Définir une feuille de route pour l'amélioration continue de la sécurité du SI.

4. Objectif général

Évaluer l'état actuel de la sécurité du SI de la SONAP et proposer des recommandations pratiques pour améliorer durablement sa résilience face aux cybermenaces.

4.1 Objectifs spécifiques :

L'audit portera sur les phases suivantes :

- **Phase 1 : Audit de la sécurité organisationnelle** et de la gouvernance
- **Phase 2 : Audit de la sécurité physique et environnementale** pour examiner la protection physique et environnementale des installations ;
- **Phase 3 : Audit de la sécurité technique** pour identifier les failles de sécurité et évaluer la robustesse des infrastructures ;
- **Phase 4 : Élaboration de recommandations et d'un plan d'action** pour améliorer la sécurité du SI ;
- **Phase 5 : Assistance pour la correction** des vulnérabilités critiques et le renforcement de la sécurité des systèmes.

5. Etendue des services et activités à assurer

L'audit couvrira les structures suivantes :
Les installations du réseau informatique, au siège de Commandayah (siège principal), de la minière (Département des Projets et la Direction des Infrastructures Pétrolières) et de Gbéssia-aéroport (où se situe la salle de visualisation sismique),

- Siège de Commandayah : DSI,
- 4 adresses IP publiques,
- 3 serveurs physiques,
- La plateforme de virtualisation (VM ware) avec échantillon de 2 VMs,
- La plateforme de sauvegarde,
- 12 Switches,

- Échantillon de 400 postes de travail de profils différents,
- 4 applications (web ou client lourd ou mobile).

Elle concernera

- La politique actuelle d'organisation et de gouvernance des SI
- Les ressources humaines SI
- Les infrastructures techniques, physiques et logicielles
- Les adresses IP publiques, les serveurs, les postes de travail, les dispositifs de sécurité, ainsi que les applications critiques.

6. Méthodologie

Description des phases :

6.1 Phase 1 : Audit de sécurité organisationnelle

Cette phase consiste à évaluer le niveau de maturité du SI en matière de sécurité organisationnelle, en comparant les pratiques actuelles aux exigences de la norme ISO 27001/2. Les aspects suivants seront examinés :

- Politique de sécurité de l'information ;
- Organisation de sécurité de l'information ;
- Gestion des actifs ;
- Sécurité liée aux ressources humaines ;
- Sécurités physiques et environnementales ;
- Exploitation et gestion des communications ;
- Acquisition, développement et maintenance des systèmes d'informations ;
- Gestion des incidents ;
- Gestion de la continuité d'activité ;
- Efficacité de l'organisation des équipes de sécurité.

6.2 Phase 2 : Audit de sécurité environnementale

L'objectif de cette phase est d'évaluer la protection physique et environnementale contre les risques humains et naturels. L'audit portera sur la sécurité physique des installations, la climatisation, l'agencement, la protection contre les incendies, le contrôle des accès physiques et les procédures d'authentification, afin de réduire les menaces de vol et de fuites d'information.

6.3 Phase 3 : Audit de sécurité technique

Cette prestation consiste à procéder à une analyse très fine de la sécurité du Système d'Information, permettant de :

- Faire apparaître les failles et les risques conséquents d'intrusions actives (tentatives de fraude, accès et manipulation illicites de données, interception de données critiques...), ainsi que celles virales ou automatisées.

- Évaluer l'herméticité des frontières du réseau, contre les tentatives d'exploitation des plates-formes de service par des attaquants externes (sites d'amplification d'attaques, relais de spam, indisponibilité de sites Web...).

- Apprécier la robustesse de la sécurité des infrastructures internet et sa capacité à préserver les aspects de confidentialité, d'intégrité, de disponibilité et d'autorisation.

- Dégager les écarts entre les procédures techniques de sécurité supposées être appliquées et celles réellement mise en œuvre.

Pour assurer cet audit technique, le titulaire est tenu d'adopter les deux scénarios de tests d'intrusions suivants, selon cet ordre :

- Scénario « boite noire » : Le titulaire procédera dans cette option à des tests techniques à distance où il ne connaît rien de la structure de la plateforme, et il procédera à des tests et analyses pour identifier et exploiter les vulnérabilités en se basant sur son bon sens et ses expériences, comme s'il était un pirate de haut niveau technique.

- Scénario « boite blanche » : Réaliser un audit intégral, en se déplaçant physiquement sur les lieux des structures à auditer. Le prestataire connaît parfaitement l'architecture et l'organisation de la plateforme.

NB : L'exploitation de n'importe quelle vulnérabilité ne doit être menée qu'après l'autorisation du Client.

NB : Les tests qui devront être réalisés ne doivent en aucun cas impacter le fonctionnement normal des applications et des systèmes en production. La période des tests devra être bien définie et limitée dans le temps.

Avant de procéder, le titulaire est tenu d'envoyer au Client une demande d'autorisation écrite mentionnant la période des tests, le (les) adresse(s) IP public source(s) (pour les tests externe).

- **Tests d'intrusion externes**

Les tests d'intrusions externes devront être réalisés depuis Internet, et prendra en charge aussi le risque d'intrusion depuis tout autre accès distant. Ces tests devront se faire avec les deux catégories suivantes (détailler ci-dessus) :

- Tests boîte noire
- Tests boîte blanche

Le prestataire devra mettre en évidence la description des failles, des vulnérabilités et leurs niveaux de criticité ainsi que les forces et les faiblesses des dispositifs mis en place. Il devra aussi décrire la démarche et les outils utilisés pour les tests d'intrusions et le scan des vulnérabilités.

Périmètre : les différentes adresses IP publiques

- **Tests d'intrusion internes**

Le prestataire retenu doit examiner la sécurité d'un échantillon, à définir lors de la phase de cadrage, de ressources SI : Serveurs, bases de données, postes de travail sélectionnés et convenus avec l'équipe de la société, identifier les vulnérabilités et leurs niveaux de criticité ainsi que les forces et les faiblesses des dispositifs mis en place sur l'ensemble de ces éléments et enfin proposer des mesures de correction.

Il devra aussi décrire la démarche et les outils utilisés pour les tests d'intrusions et les scans de vulnérabilités.

Périmètre :

- 3 serveurs physiques,
- La plateforme de virtualisation (VM ware) avec échantillon de 2 VMs,
- La plateforme de sauvegarde,
- 12 Switches,
- Échantillon de 400 postes de travail de profils différents,
- 4 applications (web ou client lourd ou mobile).

- **Audit de configuration**

L'audit de configuration des équipements vise à examiner les fichiers de configuration et vérifier leurs conformités par rapport aux =besoins de

la sécurité et aux meilleures pratiques dans le domaine afin d'identifier les faiblesses et de proposer un paramétrage sécurisé.

Il s'agit, à titre indicatif, de réaliser l'analyse au niveau des composants suivants :

- Réseau local : Equipements (pare-feu, switchs, ...), architecture interne logique, architecture de la plate-forme de sécurité (positionnement des dispositifs, plan d'adressage interne)
- Serveurs et postes de travail : mises à jour et patchs, mise à jour des systèmes d'exploitation et logiciels, bases de données, dispositifs de sécurité (antivirus, système de sauvegarde,), authentification (robustesse des mots de passe, utilisation d'authentification forte, comptes systèmes et applicatifs...), système de fichiers (droits d'accès, partages, utilisation de chiffrement...), cryptographie, services en écoute, journalisation, configuration réseau, stratégie de sécurité.
- Applications et bases de données : gestion de la traçabilité des opérations, Gestion des profils et privilèges, gestion des formats de données, cryptographie, authentification, architecture sécuritaire de déploiement, analyse de la configuration applicative et base de données, analyse de la sécurité des scripts.

  - **Audit d'architecture**

Le titulaire est chargé d'analyser l'architecture des systèmes et équipements réseaux audités, et les comparer à l'état de l'art en la matière. A travers l'audit d'architecture, le titulaire retenu doit examiner le positionnement des différents dispositifs de sécurité mis en place au niveau de notre architecture ainsi que la stratégie de sécurité sur les périmètres internes et externes.

Il devra réaliser un diagnostic de la sécurité de l'architecture du système d'information, des plateformes et solutions. Il devra définir les points faibles et forts des maillons composant la chaine applicative, recenser et qualifier les vulnérabilités et trouver les parades techniques pour y remédier.

Un design d'architecture de sécurité réseau doit être élabore et ce, en tenant compte des failles de sécurité identifiées, du dimensionnement du réseau ainsi que des nouvelles menaces auxquelles la structure informatique devrait faire face.

6.4 Phase 4 : Recommandations et plan d'actions

À l'issue des phases d'audit, des recommandations seront formulées pour adresser les dysfonctionnements, vulnérabilités et risques identifiés. Une politique de plan–d'action global sera élaborée, incluant les priorités, les responsables de mise en œuvre et les échéances.

6.5 Phase 5 : Assistance

Une assistance sera fournie pour corriger les vulnérabilités critiques identifiées et renforcer la sécurité des systèmes. Cette assistance peut inclure :

- Support pour la correction des vulnérabilités critiques ;
- Classification des actifs informationnels ;
- Analyse des risques ;
- Élaboration des procédures internes ;
- Formalisation de la politique générale de sécurité SI ;
- Investigations numériques ;
- Évaluation de la sécurité des applications avant leur mise en production.

7. Résultats attendus de la mission

Les livrables attendus pour chaque phase sont les suivants :

- **Phase 1 :** Rapport d'audit organisationnel avec constats et recommandations.
- **Phase 2 :** Rapport d'audit environnemental avec recommandations pour chaque risque identifié.
- **Phase 3 :** Rapport d'audit technique, incluant une cartographie des risques SI d'intrusion ou de cyberattaques.
- **Phase 4 :** Plan d'actions
- **Phase 5 :** Rapports d'assistance détaillant les actions réalisées à la demande

8- Durée prévisionnelle de la mission du consultant et modalités de réalisation

L'audit se déroulera sur une période de **trois mois**, avec les étapes suivantes :

- **Planification :** 1 semaine
- **Collecte de données :** 3 semaines
- **Analyse :** 5 semaines
- **Rapport préliminaire :** 1 semaine
- **Rapport final et Restitution :** 1 semaine

9- Profil du consultant (cabinet) et du personnel clé

L'équipe d'audit devra être constituée d'experts certifiés en sécurité des systèmes d'information, spécialisés en conformité réglementaire et gestion des risques informatiques.

Elle devra comprendre :

Intervenants	Profils requis	Expérience minimale
Chef de projet cybersécurité /Chef de mission	CISSP ou CCSP ET ISO 27001 LA ou LI ET CISA	Bac+5 en informatique ou équivalent + 8 ans minimum d'expérience en gestion de projets cybersécurité, gouvernance SSI et gestion des risques
Consultant senior en audit organisationnel & conformité	ISO 27001 LA et LI + CISA	Bac+5 ou équivalent + 5 ans minimum en audit SMSI, gestion des risques, contrôle interne et conformité réglementaire
Lead consultant en tests d'intrusion / audit de code	OSEP ou OSCP	Bac+5 ou équivalent + 5 ans minimum en tests d'intrusion avancés (interne, externe, applicatif, revues de code)
Consultants en tests d'intrusion / audit de code (x2)	OSCP ou CRTE	Bac+3 à Bac+5 ou équivalent + 3 à 5 ans d'expérience en pentest
Lead consultant en architecture et sécurité des systèmes	CISSP + ISO 27001 LI ou LA (CISA apprécié)	Bac+5 ou équivalent + 10 ans minimum en architecture sécurité, durcissement, revues d'architecture et gestion des risques techniques
Consultant en architecture & configuration sécurité (support)	CCSP, CISM, CEH ou ISO 27001 LI	Bac+5 ou équivalent + 5 ans minimum en audit d'architecture technique et configuration sécurisée

En plus, le Cabinet devra justifier d'une expérience avérée, d'au moins 10 ans accompagner des attestations de bonne exécution dans le domaine de l'audit de la sécurité de l'information.

10- Mode de sélection et critères d'évaluation

Les critères pour l'établissement de la liste restreinte :

Les candidats intéressés sont invités à manifester leurs intérêts pour les prestations de service ci-dessus en fournissant les informations indiquant qu'ils sont qualifiés pour exécuter les services (la nature des activités du candidat et le nombre d'années d'expérience, les qualifications du candidat dans le domaine des prestations et notamment référencées concernant des

marchés analogues; l'organisation technique et managériale du Cabinet, les qualifications générales et le nombre de l'effectif du personnel par catégorie professionnelle).

Le candidat classé premier sera invité à présenter une proposition financière. Au bout de ce processus, le consultant sera choisi selon la méthode de sélection fondée sur la qualification des consultants.

Les critères d'évaluation, et leurs poids respectifs sont les suivants :

Critères	**Points**
Nature des activités du cabinet et nombre d'années d'expérience dans le domaine de la cybersécurité et de l'audit SI	30
Qualifications du cabinet dans la réalisation de missions similaires (audit de sécurité, cybersécurité, audit SI, pentest, etc.)	20
Organisation technique et managériale du cabinet (structure, méthodologie, moyens techniques)	20
Qualifications générales du personnel clé et effectif du personnel professionnel	30

Pondération totale : 100 points

La note technique minimum T(s) requise pour être admis est : **70 Points**

Dossiers de candidature

Les cabinets intéressés devront fournir un dossier comprenant les documents suivants :

- **Une lettre de manifestation d'intérêt**, datée et signée, adressée au **Directeur Général de la Société Nationale des Pétroles (SONAP S.A.)** ;
- **Une présentation du cabinet** incluant la nature des activités et les domaines d'expertise ;
- **Les CV du personnel clé**, indiquant notamment :
  - Les formations académiques ;
  - Les expériences professionnelles ;
  - Les certifications pertinentes ;
- **Les attestations de bonne exécution ou références de missions similaires** ;
- **Un tableau récapitulatif des missions similaires réalisées**, précisant :

- Le client
- L'objet de la mission
- La durée
- Le montant du contrat
- L'année de réalisation.

La procédure de la présente manifestation d'intérêt sera conduite conformément aux dispositions des **articles 33 et 35 du Code des marchés publics.**

Les candidats intéressés peuvent obtenir des informations complémentaires auprès des adresses ci-après:

- ✓ Le Responsable de passation des Marchés Publics auprès de la Société Nationale des Pétroles Tel : 621 20 98 73 du lundi au jeudi de 8h à 16h et les vendredis de 8h à 13h.
- ✓ Le Directeur des systèmes d'information Tel : 622923537/626269906

Les manifestations d'intérêt doivent être déposées en quatre (4) exemplaires dont un (1) original et trois (3) copies à la Société Nationale des Pétroles (SONAP), sis à Minière, Commune de Dixinn, au plus tard le ...../...../2026 à 10h 00mn.

(L'ouverture des plis aura lieu le même jour à 10h 30 mn en présence des candidats qui en désireront).

Conakry, le ...../...../2026

Le Directeur Général

P/O Le Directeur Général Adjoint

Présidence de la République
Directeur Général Adjoint
Société Nationale des Pétroles SONAP

Fama Bangaly SOUMAORO