Appel d'offres pour le recrutement d'un prestataire en vue de l'audit de la sécurité informatique du système d'information de l'OAPI

TERMES DE REFERENCES

1. CONTEXTE

L'Organisation Africaine de la Propriété Intellectuelle (OAPI) est une Organisation intergouvernementale africaine spécialisée dans le domaine de la propriété intellectuelle. Elle compte à ce jour dix-sept (17) Etats membres à savoir : Bénin, Burkina Faso, Cameroun, Centrafrique, Comores, Congo, Côte d'ivoire, Gabon, Guinée, Guinée-Bissau, Guinée-Equatoriale, Mali, Mauritanie, Niger, Sénégal, Tchad et Togo.

L'OAPI dont le siège se trouve à Yaoundé, au Cameroun, a pour missions :

- la délivrance des titres de propriété industrielle ;
- la mise à disposition de la documentation et la diffusion de l'information ;
- la formation en propriété intellectuelle ;
- la contribution à la promotion de la protection de la propriété littéraire et artistique ;
- la participation au développement économique des Etats membres.

L'Organisation est l'office de propriété industrielle des 17 Etats membres. Il en résulte que toutes les procédures de délivrance des titres de propriété industrielle sont centralisées à l'OAPI et les titres délivrés sont valables dans tous les Etats membres.

Au cours de l'année 2021, L'OAPI a fait l'objet d'un audit de gestion des exercices 2018, 2019 et 2020. Ledit audit a révélé des insuffisances et faiblesses au niveau du système d'information de l'Organisation. Celles-ci portent entre autres sur :

- L'inexistence d'un processus de gestion des contenus électroniques ;
- le risque d'accès frauduleux ou malveillant aux données microsoft de l'Organisation ;
- l'absence d'une politique de sécurité informatique,
- l'absence d'une procédure de gestion des changements ;
- l'absence d'une procédure de gestion des incidents ;
- l'absence d'une procédure de gestion des sauvegardes ;
- l'absence d'un plan de reprise après sinistre ;
- la non-effectivité de la séparation des tâches entre environnement DEVELOPPEMENT et environnement PRODUCTION dans le dispositif de contrôle.

Pour corriger les faiblesses et insuffisances ci-dessus, mettre en œuvre les recommandations issues de l'audit de gestion de l'Organisation et faire une évaluation de la sécurité informatique de son système d'information en vue de garantir la maîtrise de son système informatique dans le cadre de la réalisation

de ses activités, l'OAPI sollicite l'accompagnement d'un prestataire.

2. OBJECTIF DE LA MISSION

L'objectif général du travail demandé est la réalisation d'un audit de sécurité informatique du système d'information de l'OAPI et de corriger les insuffisances et faiblesses relevées. Il s'agira notamment de détecter les failles de sécurité potentielle du système d'information de l'OAPI, d'analyser et évaluer les risques associés, et faire des recommandations.

Les prestations demandées dans le cadre de cette mission couvrent notamment les points ci-après :

L'audit organisationnel et physique,

- L'audit technique,
- L'analyse et d'évaluation du risque.

2.1. Audit organisational et physique.

Le consultant devra :

- Evaluer les aspects organisationnels de gestion de la sécurité informatique de l'OAPI
- Estimer les risques
- Proposer les recommandations pour la mise en place des mesures organisationnelles et d'une politique sécuritaire adéquate.

L'intérêt sera porté aux aspects de gestion et d'organisation de la sécurité informatique, sur les plans organisationnels, humains et physiques.

Le prestataire empruntera une approche méthodologique basée sur des batteries de questionnaires, préétablis et adaptés à la réalité de l'OAPI, permettant d'aboutir à une évaluation pragmatique des failles de sécurité.

La prise en compte des référentiels des normes éprouvées, à l'instar de ISO/IEC 27001 / 27002, dans l'approche méthodologique est recommandée.

2.2. Audit technique

Le prestataire évaluera techniquement l'architecture de sécurité du système informatique de l'OAPI. Il devra :

- Procéder à une analyse détaillée de l'infrastructure sécuritaire des composants du système informatique de l'OAPI, et tout particulièrement

son réseau ;

- Réaliser les tests d'intrusion et de vulnérabilité ; ces tests couvriront les catégories de robustesse, confidentialité, intégrité, disponibilité, authentification, certification, non répudiation et autorisation ;
- Faire émerger les failles de sécurité inhérentes aux intrusions actives.

Le prestataire réalisera des audits techniques de vulnérabilité, des tests et simulations d'attaques réelles, afin de :

- Dégager les écarts entre l'architecture de sécurité réelle et celle décrites lors des entretiens ou dans la documentation

- Dégager les écarts entre les procédures techniques de sécurité décrites (sauvegarde et restauration, PRA/PCA, etc.) et celles réellement mise en œuvre

- Evaluer la vulnérabilité des composantes matérielles et logicielles du système informatique (firewall, routeurs, reverse-proxy, switch, systèmes, mécanismes d'administration et de gestion, plates-formes matérielles, etc.), contre les principales formes de fraudes et d'attaques

- Evaluer l'étanchéité des frontières du réseau, contre les tentatives d'exploitation par des attaquants externes (sites d'amplification d'attaques, relais de spam, exploitation du PABX pour le détournement (« vol ») des lignes de communication, etc.).

Les tests réalisés ne devront pas entrainer l'interruption de service du système informatique de l'OAPI durant les périodes de production. Les tests critiques, susceptible de provoquer des effets de bord, devront être notifiés à l'OAPI pour une planification adéquate.

2.3. Analyse et d'évaluation du risque

Le prestataire partira d'une approche méthodologique décrite, pour évaluer les risques inhérents aux failles de sécurité précédemment identifiées.

L'analyse consistera, sans s'y limiter, à :

- Cartographier les ressources critiques : les informations, les actifs matériels, les actifs logiciels, les personnels, etc.
- Identifier les menaces, intentionnelle ou non, auxquels sont confrontés ces actifs

- Identifier les vulnérabilités, au niveau organisationnel, au niveau physique et au niveau technique, qui pourraient être exploitées par les menaces,
- Identifier les impacts que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs,
- Evaluer la probabilité réaliste d'une défaillance de sécurité au vu des mesures actuellement mises en œuvre.

L'évaluation consistera, sans s'y limiter, à :

- Etablir une classification des risques par niveaux, et déterminer le niveau du risque acceptable,
- Evaluer les risques, en fonction des facteurs identifiés dans la phase d'analyse, et les classifier par niveaux,
- Identifier les mesures préventives et les mesures correctives de sécurité à implémenter pour éliminer ou réduire les risques identifiés

2.4. Outils d'audit

L'utilisation d'outils commerciaux devra être accompagnée d'une licence originale et nominative, permettant leur usage correct pour de telles missions. Les outils disponibles dans le domaine du logiciel libre pourront également être utilisés.

Les outils nécessaires à la réalisation de la mission devront inclure, sans s'y limiter, les catégories fonctionnelles suivantes :

- Sondage et de reconnaissance du réseau.
- Test automatique de vulnérabilités du réseau.
- Audit des équipements réseau (switch, firewall, routeurs, reverse-proxy)
- Audit de chaque type de plateformes système (OS) présente dans l'infrastructure.
- Audit des SGBD existants.
- Test de la solidité des objets d'authentification (fichiers de mots clés, ...).
- Analyse et d'interception de flux réseaux :
- Test de la solidité des outils de sécurité réseau (firewalls, IDS, IPS, authentification).
- Scan d'existence de connexions dial-up dangereuses (war-dialing).

3. ORGANISATION DE LA MISSION

D'une manière opérationnelle, une équipe en charge du suivi de l'exécution du projet sera mise en place et coordonnée par un cadre de l'OAPI.

Au début de l'assistance, le prestataire devra produire un calendrier de travail couvrant les différentes activités prévues ci-dessus. Ce projet de calendrier sera validé par la Direction générale de l'OAPI.

Par la suite, il aura l'obligation de produire un rapport hebdomadaire montrant les progrès réalisés dans l'exécution de la mission. Le prestataire tiendra des séances de travail régulières avec l'équipe de suivi pour produire les résultats intermédiaires et les faire valider au fur et à mesure.

En fin de mission, un rapport final sera produit. Ce rapport fera ensuite l'objet d'amendements et d'observations par la Direction générale.

Le prestataire produira le document définitif comprenant les amendements de toutes les parties prenantes.

4. LIVRABLES

Le Prestataire produira les livrables suivants répondant aux objectifs de la mission :

1. Un rapport détaillé d'audit couvrant les différents aspects spécifiés dans les prestations attendus du présent terme de référence. Il devra comprendre à minima :

    - Une section relative à l'audit organisationnel et physique, fournissant l'ensemble des failles de sécurité d'ordre organisationnelle et physique ; ainsi que les recommandations y afférentes.

    - Une section relative à l'audit technique, indiquant les vulnérabilités existantes et leurs impacts sur la pérennité des systèmes d'information ; ainsi que les recommandations y afférentes.

    - Une section relative à l'analyse des risques fournissant une évaluation des risques résultant des menaces identifiées et des failles découvertes lors des phases d'audit organisationnel, physique et technique.

    - Une section relative au plan d'action et stratégie de sécurité à appliquer sur le court terme. Il comprendra des recommandations précises pour pallier aux failles et insuffisances décelées.

    - Une annexe répertoriant l'ensemble des travaux de test et d'analyse effectués dans le cadre de l'audit technique, en les ordonnant selon leurs niveaux de sévérité.

2. Un rapport présentant le plan d'action cadre, permettant de mettre en

œuvre une stratégie de sécurité cohérente et ciblée sur le moyen terme.

3. Un rapport de synthèse, destiné à la direction générale, qui inclura d'une manière synoptique les résultats de l'estimation des risques, un résumé succinct des importantes mesures organisationnelles, physiques et techniques préconisées sur le court et moyen terme, ainsi que les grandes lignes du plan d'action cadre proposé.

5. PROFIL DU PRESTATAIRE

Les prestations des présents termes de références doivent être menées par un prestataire ayant des expériences prouvées dans les différents champs d'expertise couverts par l'audit de sécurité informatique des systèmes d'informations.

Le prestataire fournira un ou plusieurs curriculums vitae détaillés, couvrant les profils ci-après :

Le chef de mission devrait justifier des qualifications suivantes :

- **Un diplôme** universitaire BAC+5 en informatique
- Dix (10) ans d'expérience en matière de gestion de projets IT
- Expérience professionnelle avérée dans l'audit de sécurité informatique des systèmes d'information
- Des compétences interpersonnelles exceptionnelles, notamment en matière de travail en équipe, de facilitation et de négociation
- De solides compétences en matière de leadership
- Excellentes aptitudes à la communication écrite et orale
- Excellentes capacités de planification et d'organisation
- Excellentes compétences analytiques et techniques.

L'expert en cybersécurité devrait justifier des qualifications suivantes :

- **Un diplôme** universitaire BAC+5 en informatique
- Huit (8) ans d'expérience dans la mise en place des systèmes de sécurité et des réseaux informatiques complexes, des méthodes d'évaluation des risques, de la sécurité des systèmes d'information, connaissance techniques en matière de détection et prévention d'intrusion, pare-feu, sauvegarde et restauration, VPN, PKI, virtualisation, cloud computing, datacenter, etc., des connaissances approfondies des différents protocoles en matière de réseau, des annuaires, messageries électroniques, systèmes d'exploitation Windows et Linux
- Avoir participé à au moins (02) missions d'audit de sécurité des systèmes d'information pour le compte d'organismes de taille similaire

- Disposer d'au moins une certification dans l'audit, à l'instar de CISA, CEH, ISO 27001 LI, ISO 27001 LA, ISO 27005, ISO 27002, etc.

6. CALENDRIER PREVISIONNEL

La durée de la mission qui se déroulera essentiellement au siège de l'Organisation situé à Yaoundé est de deux (2) mois.

7. CONTENU DES OFFRES

Les offres devront notamment contenir :

- La lettre de soumission
- Les curriculums vitæ des consultants devant effectuer la prestation incluant les références techniques et la nature des travaux similaires déjà réalisés : dates, lieux et preuves
- Un exposé décrivant de manière explicite la compréhension des besoins exprimés par l'OAPI
- Une brève description de la méthodologie de gestion de projet proposée
- L'offre financière contenant les coûts estimatifs en francs CFA

Les offres devront parvenir à l'adresse : OAPI, Place de la Préfecture Nlongkak, B.P. 887 Yaoundé - Cameroun, Tél. +237 222 20 57 00 au plus tard le XX février 2021 à 13 heures.

7. CRITERES D'EVALUATION

L'examen des critères d'évaluation va consister en une vérification de la conformité de l'offre du soumissionnaire par rapport aux exigences des termes de référence.

L'OAPI choisira librement l'offre du soumissionnaire qui lui paraîtra la meilleure au regard des critères ci-après :

N°	Critères	Note
1	Présentation générale de l'offre	/5
2	Compréhension des objectifs de la mission	/25
3	Références professionnelles du soumissionnaire	/40
4	Eléments du coût	/30
	TOTAL	100

La Direction Générale de l'OAPI se réserve le droit d'apporter toutes modifications ultérieures au présent appel d'offres ou de ne lui donner aucune suite.

La Direction Générale