Orabank

TERMES DE REFERENCE

Consultation pour le choix d'un prestataire :

LOT 1 : PENTESTS
LOT 2 : PCI-DSS

Groupe Orabank

DATE	09/12/2025
Direction	Direction Système et technologies / RSSI
Version	1.0
RSSI	

Table des matières

1. CONTEXTE ET JUSTIFICATION

Le Groupe Orabank est présent dans 12 pays d'Afrique de l'ouest et du centre. Il est organisé comme suit :

- Holding du Groupe à Lomé au Togo ;
- 12 filiales ou succursales repartis dans les pays suivants : Bénin, Burkina Faso, Côte d'Ivoire, Gabon, Guinée, Guinée Bissau, Mali, Mauritanie, Niger, Sénégal, Tchad et Togo.

Dans le cadre de ses obligations de management de la sécurité du Système d'information, le groupe envisage la poursuite des activités suivantes :

- Tests de vulnérabilités (pentests internes et externes, Scans ASV) sur tous les sites Orabank
- Accompagnement au maintien des certificats PCI-DSS dans les 12 filiales Orabank

Il est donc plus que jamais nécessaire pour Orabank de s'assurer que :

- d'une part que le système d'information ne contient pas de vulnérabilités susceptibles de l'exposer à une attaque cyber
- d'autre part que les données sensibles concernant la monétique et les produits digitaux financiers de notre institution sont sécurisées et sont aligné rapport aux exigences de la norme PCI-DSS

2. OBJECTIFS DE LA CONSULTATION

L'objectif de la consultation étant double. Il s'agit de choisir un Consultant compétents pour conduire les travaux de chacun des lots indépendants ci-dessous :

- **LOT 1 : Scans de vulnérabilités**
  Il s'agit d'effectuer pour les 12 sites et Oragroup les pentests suivants :
  - Pentests internes semestriels
  - Pentests externes semestriels

- **LOT 2 : Accompagnement au maintien de certification PCI-DSS**
  Les travaux consistent à accompagner les 12 filiales Orabank dans le cadre du maintien ou renouvellement de leur certificat PCI-DSS. En effet depuis 2021, année de leur première certification PCI-DSS, les filiales l'ont maintenu chaque année avec l'accompagnement d'un cabinet disposant de Consultants PCI-QSA (Quality Security Assessors).

La partie 3 de ce document fourni en détails les informations relatives à chaque lot ainsi que les conditions de sélection des partenaires.

3. INTERVENTION DU CONSULTANT

3.1 LOT 1 : PENTESTS

3.1.1 Objet de la consultation

Le Lot 1 a pour objet de définir les exigences relatives à la réalisation des **tests d'intrusion obligatoires dans le cadre d'un management soutenue de la sécurité du S.I et aussi la conformité PCI DSS v4.0.1**.

Les tests à réaliser concernent :

- ✓ Les **pentests externes**
- ✓ Les **pentests internes**
- ✓ Le **test de segmentation PCI DSS (CDE vs hors CDE)**
- ✓ Le **test Wi-Fi / détection de points d'accès non autorisés**

Ces prestations couvrent **les filiales du groupe** telles que détaillées dans la section suivante.

3.1.2 Périmètre des filiales concernées

Les tests d'intrusion doivent être réalisés pour :

- **Filiales Oragroup (12 filiales)**

Ces entités manipulent ou supportent des données de cartes à grande échelle et nécessitent un périmètre de test complet :

1. Bénin (OBJ)
2. Burkina Faso (OBF)
3. Côte d'Ivoire (OCI)
4. Gabon (OGA)
5. Guinée (OGN)
6. Guinée Bissau (OGW)
7. Mali (OML)
8. Sénégal (OSN)
9. Tchad (OTD)
10. Togo (OTG)
11. Mauritanie (OMR)
12. Niger (ONE)

Tests obligatoires pour chaque filiale

- 2 pentests externes par an
- 2 pentests internes par an
- 1 test de segmentation par an
- 1 test Wi-Fi par an

- **Oragroup (Siège)**

Cette entité agit comme support transversal, héberge certains composants centraux et participe à la gouvernance.

Tests obligatoires pour OGP :

- 2 pentest interne par an
- 2 pentest externe par an
- 1 test de segmentation par an

3.1.3 Fréquence des tests d'intrusion (Résumé global)

Type de filiale	Pentest externe	Pentest interne	Test segmentation	Test Wi-Fi
12 Filiales	**2 / an**	**2 / an**	**1 / an**	**1 / an**
Oragroup	**2 / an**	**2 / an**	**1 / an**	**1 / an**

3.1.4 Description détaillée des tests

- **Test d'intrusion externe**

Objectif : évaluer la résistance des services exposés à Internet.
Le prestataire doit :

- ✓ Identifier les services accessibles publiquement
- ✓ Effectuer des attaques ciblées (OWASP, OSSTMM)
- ✓ Tester l'authentification et les interfaces d'exposition
- ✓ Examiner les API et services monétiques exposés
- ✓ Réaliser une exploitation manuelle (pas uniquement automatisée)

Échantillonnage minimum

- ✓ Toutes les IP publiques correspondant au périmètre PCI DSS
- ✓ Pour les filiales Level 1 : test complet
- ✓ Pour Level 2 : test ciblé prioritaires sur environnements appli / bancaire

- **Test d'intrusion interne (réseau interne)**

Objectif : vérifier la capacité d'un attaquant interne ou d'un attaquant ayant compromis un poste à se déplacer dans le réseau.
Le test doit couvrir :

- ✓ CDE
- ✓ Réseaux utilisateurs
- ✓ Réseau d'administration
- ✓ Serveurs monétiques, HSM, applicatifs
- ✓ Mouvements latéraux

- **Test de segmentation PCI DSS**

  Test essentiel pour valider que les zones hors CDE ne peuvent pas atteindre le CDE.
  Le test doit vérifier :

- ✓ Filtrage réseau
- ✓ Cloisonnement VLAN
- ✓ ACL, règles firewall
- ✓ Absence de contournement
- ✓ Absence de connexions transitives (jumping)

  Résultat attendu : "Segmentation effective" ou "Non conforme"

- **Test Wi-Fi / détection des Rogue Access Points**

  Objectif : s'assurer que :

- ✓ Aucun réseau Wi-Fi non autorisé n'est connecté au réseau PCI
- ✓ Aucun point d'accès non déclaré n'est présent
- ✓ Les réseaux autorisés sont sécurisés (WPA2/WPA3 – clé forte – absence de bridage vers CDE)
- ✓ Le prestataire réalise :
- ✓ Balayage sur site
- ✓ Tentative d'association
- ✓ Vérification des protections cryptographiques
- ✓ Tests de pont Wi-Fi → LAN

3 .1.5 Méthodologie exigée

Le prestataire doit respecter :

- ✓ PCI DSS v4.0.1 – Exigence 11.3
- ✓ OSSTMM (méthodologie principale)
- ✓ OWASP (Web / API / Mobile)
- ✓ NIST SP800-115
- ✓ Tests manuels obligatoires
- ✓ Retests systématiques
- ✓ Respect strict des Rules of Engagement (ROE)

3.1.6 Livrables attendus

Pour chaque filiale :

- ✓ Rapport technique détaillé (vulnérabilités, preuves, exploitation)
- ✓ Rapport exécutif (management)
- ✓ Matrice de risque (CVSS v3.1)
- ✓ Rapport de segmentation
- ✓ Rapport Wi-Fi
- ✓ PV de retest

Les livrables doivent être fournis **séparément pour chaque filiale + un rapport consolidé groupe**.

3.1.7 Contraintes & obligations

- ✓ Respect strict de la norme PCI DSS v4.0.1
- ✓ Disposer de consultants certifiés (OSCP, CEH, ISO 27001, PCI QSA).
- ✓ Confidentialité et signature NDA
- ✓ Respect des délais et participation aux comités projet
- ✓ Preuves échangées via canaux sécurisés

3.1.8 Conditions financières et logistiques

- **Déplacements**

Tous les **déplacements, hébergements et frais logistiques** nécessaires pour les interventions sur site sont **entièrement à la charge du prestataire**.

- **Conditions de soumission et délais**

Le prestataire souhaitant répondre au présent cahier de charge doit justifier de l'expertise nécessaire pour la réalisation des différentes missions qui y sont demandées, et de ce fait :

Le prestataire retenu devra satisfaire à l'ensemble des critères suivants :

- Avoir des références en ayant conduit des missions similaires, et certifié des banques, avec au moins 5 références.
- Disposer des Consultants certifiés ISO27001 LA/LI , CISM ,27005 RM, OSCP,CISSP,CEH ou équivalents.
- Être un soumissionnaire accrédité PCI QSA.
- Disposer d'au moins 2 consultant certifié PCI QSA

Afin de justifier de l'expérience exigée, le prestataire et tenu de fournir les attestations justificatives signées par les concernés par ces missions de références.
Pour tout document ou attestation manquant, le dossier du prestataire sera considéré comme incomplet et pourrait être rejeté.

- **Démarche d'évaluation**

La procédure de jugement des offres se déroulera comme suit :

- **Phase 1 : évaluation des candidats et des offres techniques :**

  Sur la base de l'offre technique, la commission d'ouverture des plis évaluera la capacité de chaque Concurrent retenu.
  Le jugement de l'offre technique prendra en considération les seuls moyens humains, techniques et logistiques dédiés à l'exécution des Services.
  La commission technique évaluera chaque offre technique sur la base de la conformité aux termes de référence, à l'aide des critères d'évaluation et du système de points spécifiés ci-après. Chaque proposition conforme se verra attribuer un score technique. Toute proposition qui ne satisfait pas à des éléments importants des termes de référence, ou n'atteint pas le score technique minimum, fixé à 170 points, sera éliminée.

  L'Offre Technique sera notée sur **200** points en prenant en considération les critères suivants :

Qualité du prestataire : sur 100 points

Critères de Notation	**Détail Critère**	**Documents servant de base pour la notation**	**Barrême**
Qualification du prestataire : sur 100 points			
Expérience et Références du prestataire dans les missions similaires	Le soumissionnaire doit disposer : • **De l'accréditation QSA** • **D'au moins 5 ans d'expérience en tant que Cabinet spécialisé en sécurité de l'information** • **Au moins cinq (5) références similaires avec certification, dont 2 pour des banques** • **Auditeur QSA**	• Accréditation QSA (10 points) : Obligatoire. • 5 Attestations de référence pour des projets similaires (dont 2 bancaires) (5 pts / réf.) • Autres attestations de référence • Auditeurs QSA 2 QSA : 15 pts ; < 2 QSA : 5 pts	50
Dispositif de Sécurité de l'information du Prestataire	Le soumissionnaire doit justifier des dispositifs déployés pour assurer la sécurité des informations sensibles : • **Certification ISO 27001** • **Certification ISO 9001** • **Conformité sur la protection des données personnelles (Loi 09-08, …)** • **PASSI**	1- Certificat ISO 27001 : 10 points 2- Certificat ISO 9001: 10 points	20

Démarche et conformité aux bonnes pratiques	Le soumissionnaire doit démontrer sa maitrise et sa capacité à accompagner sur les prestations objet du présent marché.	• Démarche exhaustive et adaptée au contexte et besoin	30

<u>Qualité de l'équipe proposée : sur 100 points</u>

Le soumissionnaire doit fournir les copies des diplômes et certificats.

Catégorie d'intervenant	**Critère d'évaluation**	**Barème (max)**	**Approche pour l'évaluation**
1Experts Cybersécurité (34)	Nombre d'années d'expérience dans le domaine de la prestation en cours	7	>14 ans : 7 points] 10 – 14] ans : 04 points < 10 ans : 0 points
	Nombre de missions réalisées dans le domaine de la prestation en cours	7	>30 : 07 points] 20 – 30] : 03 points < 20 : 0 points
	Certifications	20	ISO 27001 Master : **4 points** CISA / CISSP : **4 points** ISO 27001 LI / LA : **3 points** ISO 22301 LA : **3 points** ISO 27005 / ISO 31000 **: 3 points** ISO27001 Senior Lead Auditor : **3 points** Les profils proposés doivent disposer d'au moins **quatre** certifications parmi la liste précitée ; Cas non échéant : **0 point**
2 Consultants & Expert cybersécurité technique (26)	Nombre d'années d'expérience dans le domaine de la prestation en cours	7	>12 ans : 5 points] 8 – 12] ans : 02 points < 8 ans : 0 points
	Nombre de missions réalisées dans le domaine de la prestation en cours	7	>20 : 5 points] 15 – 20] : 02 points] 5 – 15] : 1 point(s)
	Certifications	12	OSCP ou équivalent : 6 points CEH ou équivalent : 6 points

Catégorie d'intervenant	Critère d'évaluation	Barème (max)	Approche pour l'évaluation
1 Chef de mission & QSA (40)	Nombre d'années d'expérience dans le domaine de la prestation en cours	10	>15 ans : 10 points] 10 – 15] ans : 5 points >10 ans : 0 points
	Nombre de missions réalisées dans le domaine de la prestation en cours	10	>15 : 10 points] 5 – 15] : 05 points < 5 : 0 points
	Certifications	20	PCI QSA : **5 points** Prince 2 / PMP / PMITS : **3 points** ISO 27001 LI / LA : **3 points** ISO 27005 / ISO 31000: **3 points** CEH / OSCP: **3 points** ITIL / ISO20000**: 1 points** Le profil proposé doit être QSA et disposer d'au moins **cinq** certifications parmi la liste précitée et d'un certificat en gestion de projet ; Cas non échéant : **0 point**

- **Phase 2 : évaluation des offres financières :**

  Après élimination des offres non retenues à l'issue de la phase 2 (offres n'ayant pas obtenu un score minimum de 170 points), il sera donné à chaque offre une valeur (Ni) selon la pondération suivante :

  - ✓ Ni= (80 x Ti + 20 x Fi) /100
  - ✓ Fi= (Pm/Pi) x 100
  - ✓ Ti : note technique obtenue par le soumissionnaire telle que déterminée à la phase 2 susvisée
  - ✓ Fi : note financière
  - ✓ Pm : prix moyen offert par les soumissionnaires
  - ✓ Pi : prix offert par le soumissionnaire

- **Phase 3 : évaluation finale des offres**

  La commission établira un état comparatif des offres tenant compte de la notation de chaque offre.

A l'issue de cette phase une note technique sera attribuée aux candidats retenus qui sera la somme des notes attribuées par critère.
Seront écartées à l'issue de l'évaluation technique les offres qui n'obtiendront pas 170 points ou plus, et celles qui obtiendront, le cas échéant, une note 0 sur l'un des critères, ainsi que celles qui ne respecteront pas l'une des exigences suivantes :

3.2 LOT 2 : PCI-DSS

3.2.1 Object de la consultation LOT 2

Ce lot a pour objet de définir les modalités techniques, fonctionnelles et organisationnelles relatives à l'accompagnement du Groupe Oragroup dans la mise en conformité et le renouvellement de la certification PCI DSS v4.0.1, couvrant l'ensemble des filiales, concernées, y compris :

- Audit, remédiation, pilotage
- Certification officielle PCI DSS (RoC, AoC, CoC)

3.2.2 Contexte et périmètre de la prestation

Oragroup est groupe bancaire panafricain implanté dans l'espace UEMOA, la CEMAC, en Guinée et en Mauritanie. Il opère des activités monétiques nécessitant la conformité aux standards PCI DSS.

Le périmètre comprend :

- Les filiales du Groupe Orabank manipulant ou impactant les données de titulaires de cartes.
- Les composantes CDE (Cardholder Data Environment) : systèmes, réseaux, personnes, processus, tiers et locaux.
- Les travaux organisationnels, techniques, tests requis par PCI DSS et le processus complet de certification.

Les filiales concernées sont :

Service Provider – Level 1 (10 filiales) :

1. Bénin (OBJ)
2. Burkina Faso (OBF)
3. Côte d'Ivoire (OCI)
4. Gabon (OGA)
5. Guinée (OGN)
6. Guinée Bissau (OGW)
7. Mali (OML)
8. Sénégal (OSN)
9. Tchad (OTD)
10. Togo (OTG)

Service Provider – Level 2 (2 filiales) :

11. Mauritanie (OMR)
12. Niger (ONE)

Filiale spécifique Groupe (OGP) :

Incluse dans le périmètre organisationnel & transverse.

3.2.3 Description des prestations

Les offres techniques devront mettre en évidence :

- La méthodologie du prestataire pour réaliser la mission
- Le phasage du projet et le planning d'intervention
- La répartition de charge pour chaque profil et le chronogramme d'intervention
- Le dispositif de pilotage et d'assurance qualité

La prestation devra inclure les activités décrites ci-dessous. Le prestataire peut proposer un autre phasage pertinent, sous réserve d'inclure l'ensemble des objectifs et livrables attendus. Les prestataires sont invités à compléter dans leurs offres les activités et livrables pertinents et indispensables à la réalisation des objectifs ci-dessus mentionnés, tout en prenant en compte l'évolution du contexte sur la dernière année.

3.2.4 Prestations attendues

Phase 0 – Cadrage et préparation
- Réunion de lancement & cadrage
- Revue documentaire (politiques, procédures, standards de configuration, etc.)
- Formation PCI DSS Lead Implementer
- Définition du périmètre PCI DSS & CDE
- Plan d'assurance qualité & plan projet

Phase 1 – Diagnostic PCI DSS
- Entretiens & visites de site
- Collecte et analyse de preuves
- Évaluation PCI DSS v4.0.1
- Rapport de diagnostic + Plan de remédiation priorisé
- Matrice CDM (Card Data Matrix)

Phase 2 – Remédiation
Organisationnelle :
- Ateliers de support pour politiques, procédures et guides
- Analyse de risque ciblée PCI DSS
- Revue PCI DSS d'un tiers
- Validation des contrôles compensatoires (CCW)
- Mise en conformité documentaire

Technique :
- Revue d'architecture & segmentation
- Scans (ASV)
- Définition des besoins technologiques (cahiers des charges)
- Assistance à la mise en œuvre

Phase 3 – Certification PCI DSS
- Audit à blanc
- Collecte finale des preuves
- Audit de certification PCI DSS (ROC/AoC/CoC)
- Préparation du package pour le PCI SSC
- Plan de maintien annuel en conformité

3.2.5 Livrables
- Plan projet & PAQ
- Supports de formation + attestations
- Rapport de diagnostic PCI DSS
- Plan de remédiation priorisé
- Manuel PCI DSS & corpus documentaire
- Scans ASV
- ROC, AoC, CoC
- PV de mission

3.2.6 Contraintes & obligations

- Respect strict de PCI DSS v4.0.1
- Confidentialité et signature NDA
- Respect des délais et participation aux comités projet
- Preuves échangées via canaux sécurisés

3.2.7 Conditions financières et logistiques

Tous les **déplacements, hébergements et frais logistiques** nécessaires pour les interventions sur site (missions cadrage, diagnostic, certification, visites DC/agences, ateliers) sont **entièrement à la charge du prestataire**.

3.2.6 Conditions de soumission et délais

Le prestataire souhaitant répondre au présent cahier de charge doit justifier de l'expertise nécessaire pour la réalisation des différentes missions qui y sont demandées, et de ce fait :

Le prestataire retenu devra satisfaire à l'ensemble des critères suivants :

- Être un soumissionnaire accrédité PCI QSA.
- Avoir des références en ayant conduit des missions similaires, et certifié des banques, avec au moins 5 références.
- Disposer d'au moins 2 consultant certifié PCI QSA
- Disposer d'au moins 2 Consultants certifiés ISO27001 LA/LI ou CISM ou 27005 RM.

Afin de justifier de l'expérience exigée, le prestataire et tenu de fournir les attestations justificatives signées par les concernés par ces missions de références.
Pour tout document ou attestation manquant, le dossier du prestataire sera considéré comme incomplet et pourrait être rejeté.

3.2.7 Démarche d'évaluation

La procédure de jugement des offres se déroulera comme suit :

- **Phase 1 : évaluation des candidats et des offres techniques :**

  Sur la base de l'offre technique, la commission d'ouverture des plis évaluera la capacité de chaque Concurrent retenu.
  Le jugement de l'offre technique prendra en considération les seuls moyens humains, techniques et logistiques dédiés à l'exécution des Services.
  La commission technique évaluera chaque offre technique sur la base de la conformité aux termes de référence, à l'aide des critères d'évaluation et du système de points spécifiés ci-après.
  Chaque proposition conforme se verra attribuer un score technique. Toute proposition qui ne satisfait pas à des éléments importants des termes de référence, ou n'atteint pas le score technique minimum, fixé à 170 points, sera éliminée.

  L'Offre Technique sera notée sur **200** points en prenant en considération les critères suivants :

Qualité du prestataire : sur 100 points

Critères de Notation	Détail Critère	Documents servant de base pour la notation	Barrême
Qualification du prestataire : sur 100 points			
Expérience et Références du prestataire dans les missions similaires	Le soumissionnaire doit disposer : • **De l'accréditation QSA** • **D'au moins 5 ans d'expérience en tant que Cabinet spécialisé en sécurité de l'information** • **Au moins cinq (5) références similaires avec certification, dont 2 pour des banques** • **Auditeur QSA**	• Accréditation QSA (10 points) : Obligatoire. • 5 Attestations de référence PCI DSS (dont 2 bancaires) (5 pts / réf.) • Autres attestations de référence • Auditeurs QSA pour le projet 2 QSA : 15 pts ; < 2 QSA : 5 pts	50
Dispositif de Sécurité de l'information du Prestataire	Le soumissionnaire doit justifier des dispositifs déployés pour assurer la sécurité des informations sensibles : • **Certification ISO 27001** • **Certification ISO 9001** • **Conformité sur la protection des données personnelles (Loi 09-08, …)** • **PASSI**	3- Certificat ISO 27001 : 10 points 4- Certificat ISO 9001: 10 points	20
Démarche et conformité aux bonnes pratiques	Le soumissionnaire doit démontrer sa maitrise et sa capacité à accompagner sur les prestations objet du présent marché.	• Démarche exhaustive et adaptée au contexte et besoin	30

Qualité de l'équipe proposée : sur 100 points

Le soumissionnaire doit fournir les copies des diplômes et certificats.

Catégorie d'intervenant	Critère d'évaluation	Barème (max)	Approche pour l'évaluation
	Nombre d'années d'expérience dans le domaine de la prestation en cours	10	>15 ans : 10 points] 10 – 15] ans : 5 points >10 ans : 0 points
	Nombre de missions réalisées dans le domaine de la prestation en cours	10	>15 : 10 points] 5 – 15] : 05 points < 5 : 0 points

Catégorie d'intervenant	Critère d'évaluation	Barème (max)	Approche pour l'évaluation
1 Chef de mission & QSA (40)	Certifications	20	PCI QSA : **5 points** Prince 2 / PMP / PMITS : **3 points** ISO 27001 LI / LA : **3 points** ISO 27005 / ISO 31000: **3 points** CEH / OSCP: **3 points** ITIL / ISO20000**: 1 points** Le profil proposé doit être QSA et disposer d'au moins **cinq** certifications parmi la liste précitée et d'un certificat en gestion de projet ; Cas non échéant : **0 point**
1Experts Cybersécurité organisationnelle (34)	Nombre d'années d'expérience dans le domaine de la prestation en cours	7	>14 ans : 7 points] 10 – 14] ans : 04 points < 10 ans : 0 points
	Nombre de missions réalisées dans le domaine de la prestation en cours	7	>30 : 07 points] 20 – 30] : 03 points < 20 : 0 points
	Certifications	20	ISO 27001 Master : **4 points** CISA / CISSP : **4 points** ISO 27001 LI / LA : **3 points** ISO 22301 LA : **3 points** ISO 27005 / ISO 31000 **: 3 points** ISO27001 Senior Lead Auditor : **3 points** Les profils proposés doivent disposer d'au moins **quatre** certifications parmi la liste précitée ; Cas non échéant : **0 point**
2 Consultants & Expert cybersécurité technique (26)	Nombre d'années d'expérience dans le domaine de la prestation en cours	7	>12 ans : 5 points] 8 – 12] ans : 02 points < 8 ans : 0 points
	Nombre de missions réalisées dans le domaine de la prestation en cours	7	>20 : 5 points] 15 – 20] : 02 points] 5 – 15] : 1 point(s)
	Certifications	12	CISM: 4 points CISSP : 3 points ISO27001 LI/LA /: 3 point(s) Certification Réseau NSE7 ou équivalent : 2 points Les profils proposés doivent disposer d'au moins **trois** certifications parmi la liste précitée ; Cas non échéant : **0 point**

- **Phase 2 : évaluation des offres financières :**

  Après élimination des offres non retenues à l'issue de la phase 2 (offres n'ayant pas obtenu un score minimum de 170 points), il sera donné à chaque offre une valeur (Ni) selon la pondération suivante :

  - ✓ Ni= (80 x Ti + 20 x Fi) /100
  - ✓ Fi= (Pm/Pi) x 100
  - ✓ Ti : note technique obtenue par le soumissionnaire telle que déterminée à la phase 2 susvisée
  - ✓ Fi : note financière
  - ✓ Pm : prix moyen offert par les soumissionnaires
  - ✓ Pi : prix offert par le soumissionnaire

- **Phase 3 : évaluation finale des offres**

  La commission établira un état comparatif des offres tenant compte de la notation de chaque offre.

A l'issue de cette phase une note technique sera attribuée aux candidats retenus qui sera la somme des notes attribuées par critère.
Seront écartées à l'issue de l'évaluation technique les offres qui n'obtiendront pas 170 points ou plus, et celles qui obtiendront, le cas échéant, une note 0 sur l'un des critères, ainsi que celles qui ne respecteront pas l'une des exigences suivantes :

4. DEMANDE D'ECLAIRCISSEMENTS

Toute demande d'informations complémentaires concernant à la présente consultation doit être adressée par écrit aux trois adresses mails suivantes :

gado.sonhaye@orabank.net

amos.tossavi@orabank.net

La demande doit leur parvenir au moins trois jours avant la date de clôture des soumissions.

Les réponses fournies par écrit prendront la forme d'additifs aux documents de la consultation et seront communiquées à l'ensemble des Consultants ayant reçu le dossier de consultation.

Les explications ou instructions fournies oralement n'ont aucune valeur contractuelle.

5. REMISE ET CONTENU DES OFFRES

5.1 Remise des offres

Les offres doivent parvenir au plus tard **le 30 janvier 2026 à 18h00 GMT** précises p**ar mail** à l'adresse mail suivante :

offre.commerciale@orabank.net

5.2 Contenu des offres

L'offre du soumissionnaire doit pour chaque Lot (LO1, LOT2) comprendre deux parties distinctes :

- **Partie I : Offre technique**
  Le soumissionnaire y présentera sa structure notamment ses activités en rapport avec le thème traité par les présents TDR.
  Il mentionnera et justifiera toutes les informations concernant permettant e l'évaluer sur la base des critères fournis dans chacun de slots auquel il soumissionne

- **Partie II : Offre Financière**

Le soumissionnaire donnera son offre de coût global (y compris les débours) et détaillé, libellé en FCFA en HT et TTC.