



Consultation pour

Audit sécurité des systèmes

d'information & tests d'intrusion

Auteurs:	VIVALIS SALAF
Référence :	AO_AUDIT_SECURITE_SI_122025
Version :	2
Statut :	Projet
Date :	26/01/2026

SOMMAIRE

1.	INTRODUCTION
2.	OBJET DE LA PRESENTE CONSULTATION.....
3.	DESCRIPTION DU PERIMETRE DE LA MISSION
3.1.	TESTS D'INTRUSION.....
3.1.1.	TESTS D'INTRUSION INTERNES
3.1.2.	TESTS D'INTRUSION EXTERNES.....
3.2.	AUDIT DE L'ARCHITECTURE TECHNIQUE.....
3.3.	AUDIT APPLICATIF
4.	Livrables
5.	REGLEMENT DE LA CONSULTATION
5.1.	OBJET DU REGLEMENT DE LA CONSULTATION.....
5.2.	DEFINITIONS
5.3.	PRESENTATION ET JUGEMENT DES OFFRES.....
7.3.1.	DOSSIER ADMINISTRATIF.....
7.3.2.	DOSSIER TECHNIQUE
7.3.3.	OFFRE TECHNIQUE.....
7.3.4.	OFFRE FINANCIERE
5.4.	ENVOI OU DEPOT DES PROPOSITIONS.....
5.5.	EXAMEN DES OFFRES
5.5.1.	L'EXAMEN DES OFFRES.....
5.5.2.	LA PROCEDURE DE JUGEMENT DES OFFRES
5.5.3.	COUT DE L'APPEL D'OFFRES
5.5.4.	DEMANDE DE RENSEIGNEMENT
5.5.5.	MODIFICATIONS AU CAHIER DES CHARGES
5.5.6.	MODIFICATION DES PROPOSITIONS.....
5.5.7.	DUREE DES ENGAGEMENTS
5.5.8.	PENALITE DE RETARD
6.	ANNEXES

CAHIER DES CHARGES

**Audit de la Sécurité du Système
d'Information & Tests d'intrusion**

1. Introduction

VIVALIS SALAF, filiale du Groupe Banque Populaire spécialisée dans le crédit à la consommation, lance la présente consultation afin de sélectionner un prestataire qualifié pour la réalisation d'un **audit de sécurité des systèmes d'information et de tests d'intrusion**.

Cette mission s'inscrit dans une démarche stratégique visant à renforcer la résilience du SI, assurer sa conformité aux normes internationales et aux exigences réglementaires marocaines, et garantir une protection optimale des données et des services critiques.

2. Objet de la consultation

La mission confiée au prestataire retenu portera sur l'évaluation des aspects **organisationnels** et **techniques** liés à la sécurité des systèmes d'information de VIVALIS SALAF.

Le périmètre couvre principalement :

- **Les tests d'intrusion** (internes et externes)
- **L'audit de l'architecture technique**
- **L'audit applicatif**

3. Description du périmètre de la mission

3.1. Tests d'intrusion

Élément	Description
Objectif	Identifier, exploiter et documenter les vulnérabilités présentes dans le SI de VIVALIS SALAF. - OWASP Testing Guide v4/v5 (applications Web) - OWASP API Security Top 10 (APIs) - PTES – Pénétration Testing Exécution Standard (infrastructure interne/externe) - NIST SP 800-115 (méthodologie générale) - CVSS v3.1 (notation des vulnérabilités) - Référentiel européen « DORA » - PASSI certification
Référentiels obligatoires	- Rapport détaillé (vulnérabilités, impact, criticité, preuves, risques, recommandations) - Livrable BANK AL-MAGHRIB - Retest post-remédiation - Journal des actions d'exploitation
Livrables attendus	Black-box, Grey-box ou White-box selon le périmètre avec et sans authentification
Approches de test	

3.1.1. Tests d'intrusion internes

Simulation d'un attaquant disposant d'un accès légitime ou illégitime au réseau interne.
Couverture minimale :

Élément	Description
Objectif	<p>Évaluer la sécurité du réseau interne en simulant l'action d'un attaquant disposant d'un accès légitime ou illégitime (employé, prestataire, invité). À travers trois étapes :</p> <ul style="list-style-type: none">• Boite noire• Boite grise• Boite blanche
Couverture minimale	<ul style="list-style-type: none">- Énumération et exploitation du réseau interne- Tests des protocoles- Évaluation Active Directory- Identification de vulnérabilités systèmes et applicatives internes- Tentatives d'élévation de privilèges (locales et domaine)- Analyse des segments réseau et cloisonnements- Recherche de données sensibles en clair- Évaluation des postes utilisateurs inclus dans le périmètre
Obligations du prestataire	<ul style="list-style-type: none">- Préciser les outils utilisés (sans détails techniques sensibles)- Décrire la méthodologie d'exploitation- Garantir l'absence d'impact opérationnel- Livraison de la synthèse post clôture phase d'audit

3.1.2. Tests d'intrusion externes

Simulation d'attaques depuis Internet. Couverture minimale :

Élément	Description
Objectif	<p>Évaluer la résistance des services exposés à Internet face à des attaques externes (non authentifiées ou authentifiées si prévu) et aussi la performance de notre WAF & nos Firewalls. À travers deux étapes :</p> <ul style="list-style-type: none">• Boite noire• Boite grise
Couverture minimale	<ul style="list-style-type: none">- Analyse des adresses IP publiques et services exposés- Tests sur applications Web exposées- Tests sur APIs exposées- Vérification TLS/SSL- Tests d'authentification/autorisation- Vulnérabilités classiques (injections, XSS, CSRF, SSRF, RCE, etc.)- Analyse configurations périphériques (firewall, WAF)- Site web

Obligations du prestataire	<ul style="list-style-type: none"> - Fournir la liste des URL, IP et services concernés (validation par VIVALIS SALAF) - Indiquer les comptes d'accès fournis le cas échéant (tests Grey-box) - Non utilisation du DDOS ou toutes tentatives de deni de service sans la validation de vivalis.
-----------------------------------	---

3.2. Audit de l'architecture technique

Critère	Description
Objectif	<ul style="list-style-type: none"> • Évaluer la robustesse, • La conformité et la résilience du SI ainsi que le niveau de sécurité des infrastructures et solutions déployées de VIVALIS SALAF.
Référentiels et standards	<ul style="list-style-type: none"> • ISO/IEC 27001 :2022 & 27002 :2022 ; • CIS Controls v8 ; • NIST CSF ; • Benchmarks CIS (serveurs, OS, équipements réseau).
Périmètre	<ul style="list-style-type: none"> • Architecture réseau ; • Infrastructures systèmes ; • Équipements et solutions de sécurité ; • Protection des postes utilisateurs ; • Services techniques et configurations critiques.
Méthodologie	<ul style="list-style-type: none"> • Démarche structurée d'analyse, • D'évaluation et de validation de l'architecture technique et des mécanismes de défense en profondeur.
Résultats et livrables	<ul style="list-style-type: none"> • Évaluation de la cohérence de l'architecture ; • Identification des vulnérabilités et écarts ; • Analyse de la défense en profondeur ; • Plan de remédiation priorisé.

3.3. Audit applicatif

Critère	Description
Objectif	<p>Évaluer le niveau de sécurité, de maturité et de conformité des applications exploitées par VIVALIS SALAF /</p> <ul style="list-style-type: none">▪ Applications métiers,▪ Solutions sur mesure,▪ Progiciels intégrés,▪ Portails et services exposés.
Couverture applicative	Prise en compte de quatre plateformes métiers (Interne, Exposé, Critique, Support) : L'objectif est de faire un état des lieux des principales solutions utilisées au niveau de l'entreprise.
Analyse sécurité	<ul style="list-style-type: none">▪ Identification des vulnérabilités potentielles,▪ Failles de conception,▪ Erreurs de configuration et risques applicatifs.
Processus et gouvernance	Analyse des processus de développement, d'intégration, de déploiement, de maintenance ainsi que des compétences et de la gouvernance applicative.
Livrables et plan d'amélioration	<ul style="list-style-type: none">▪ Rapport de sécurité applicative▪ Analyse fonctionnelle et opérationnelle▪ Analyse des processus de développement, intégration et déploiement▪ Recommandations et plan d'amélioration

3.4. Délais de mise en production

Mission	Délai maximal	Point de départ du délai	Livrables inclus
Tests d'intrusion	4 semaines	Notification du bon de commande ou signature du contrat	Rapports internes, externes, applicatifs + Rapport Bank Al-Maghrib
Audit d'architecture SI	1 mois	Après finalisation du projet de refonte réseau & sécurité (fin T1 2026)	Rapport complet d'audit d'architecture

3.5. Exigence réglementaire DGSSI

Le prestataire doit être **agrémenté ou autorisé par la DGSSI** pour réaliser des missions d'audit et de tests d'intrusion au Maroc.

✓ **Pièces obligatoires à fournir :**

- Copie officielle de l'autorisation/agrément DGSSI valide
- Liste des consultants autorisés par la DGSSI (minimum un auditeur senior)
- Confirmation du périmètre d'intervention autorisé (audit technique, Pentest, cybersécurité)

Ref	Exigence	Obligation
T1	Agrément DGSSI Maroc	Éliminatoire
T2	Équipe déclarée DGSSI (minimum un auditeur senior)	Obligatoire
T3	Chef de projet certifié ISO 27001 LA	Obligatoire
T4	Pentesters certifiés (OSCP ou CEH ou eCPPT ou GPEN)	Obligatoire
T5	Méthodologie documentée	Obligatoire

**** Obligations Fonctionnelles Contractuelles :**

Ref	Exigence	Statut
F1	Tests d'intrusion internes, externes et applicatifs	Obligatoire
F2	Retest après remédiation	Obligatoire
F3	Rapports & plans d'action	Obligatoire
F4	Respect des méthodologies internationales (OWASP, NIST, ISO, CIS)	Obligatoire
F5	Respect des délais contractuels	Obligatoire

4. Livrables

Livrable	Contenu	Objectif
Rapports Penteste : <ul style="list-style-type: none"> • Tests d'intrusion internes • Tests d'intrusion externes • Tests applicatifs 	Résultats des tests d'intrusion internes, externes et applicatifs applications	Identifier vulnérabilités et risques exploitables
Rapport architecture	Analyse de l'architecture SI (réseau, serveurs, applications, flux)	Évaluer robustesse, résilience et conformité
Plan d'actions détaillé à réaliser à court, moyen et long terme avec le degré de sensibilité de chaque action	Liste des mesures correctives classées par priorité Avec investissements/charges nécessaires (à estimer)	Suivre et corriger efficacement les vulnérabilités
Matrice CVSS	Tableau des vulnérabilités avec scores CVSS	Prioriser les actions selon la gravité des risques
Journal exploitation tests	Enregistrement détaillé des tests réalisés	Assurer traçabilité et reproductibilité des audits
Re-Test	Vérification post-correctifs des vulnérabilités	Valider l'efficacité des mesures mises en œuvre
Rapport Bank Al-Maghrib	Rapport conforme aux exigences réglementaires	Garantir la conformité et informer les autorités

REGLEMENT DE LA CONSULTATION

Audit de la Sécurité du Système

d'Information & Tests d'intrusion

5. REGLEMENT DE LA CONSULTATION

5.1 Objet du règlement de la consultation

Le présent règlement concerne la consultation relative au choix d'un prestataire pour la mission d'Audit de la sécurité des systèmes d'information et tests d'intrusion

5.2 Définitions

Il sera attribué aux termes rencontrés dans ce document les significations suivantes :

- « L'Entreprise » désigne la firme, le cabinet ou la société du prestataire, participant à la concurrence pour la réalisation de la prestation d'Audit de la sécurité des systèmes d'information et tests d'intrusion.
- La « Commission » désigne la commission de jugement des offres constituée par VIVALIS SALAF.
- L'« Adresse » de VIVALIS SALAF fait référence à l'adresse suivante :

Organisme adjudicateur : **VIVALIS SALAF**

Autorité compétente : **Secrétariat de la Direction Générale**

Adresse : **369, Boulevard Zerkouni**

Ville : **CASABLANCA**

5.3 Présentation et jugement des offres

L'Entreprise est tenue de présenter dans une première enveloppe fermée une offre comprenant un dossier administratif et technique, dans une deuxième enveloppe fermée une offre technique et dans une troisième une offre financière, le tout dans un seul pli fermé et scellé, transmis à l'adresse de VIVALIS SALAF.

Chaque pli doit être cacheté et porter :

- Le nom et l'adresse de l'Entreprise ;
- L'objet du marché ;
- La mention « ce pli ne doit être ouvert que par le Président de la Commission des marchés lors de la séance d'examen des offres ».

5.3.1 Dossier Administratif

Le dossier administratif doit comprendre :

- La déclaration sur l'honneur prescrite en double exemplaires suivant le modèle joint en annexe I. Cette déclaration doit indiquer également :
 - L'attestation RC/modèle J,
 - Le numéro de patente,
 - L'identifiant fiscal,
 - Le numéro d'affiliation à la Caisse Nationale de Sécurité Sociale,
 - Le numéro du compte courant postal, bancaire ou du Trésor, du soumissionnaire.
- Les pouvoirs conférés à la personne agissant au nom du soumissionnaire ;

- Une attestation de pouvoir au cas où le soumissionnaire serait associé à un autre pour la réalisation du présent projet ;
- Une attestation délivrée depuis moins d'un an par le percepteur du lieu d'imposition certifiant que le soumissionnaire est en situation fiscale régulière. Cette attestation doit mentionner l'activité au titre de laquelle le soumissionnaire est imposé ;
- Une attestation délivrée depuis moins d'un an par la CNSS certifiant que le soumissionnaire est en situation régulière envers cet organisme.
- Une Attestation pluriannuelle de la CNSS avec masse salariale annuelle et nombre moyen d'employés en CDI.
- Les Bilans des 3 derniers années, appuyés par une attestation de chiffres d'affaires déclarés délivrée par l'administration des impôts.

5.3.2 Dossier Technique

Le dossier technique contiendra les éléments suivants :

- Une note indiquant les moyens humains et techniques du soumissionnaire,
- Une note de présentation du soumissionnaire marocain ou étranger, partenaire technique ou associé, le cas échéant, ainsi que la part des travaux qui lui seront confiés et les profils des intervenants.
- Le présent cahier des charges dûment paraphé et signé par le (s) soumissionnaire (s) avec la mention « lu et approuvé ».

5.3.3 Offre Technique

Cette offre contiendra les éléments suivants :

- Une note présentant la démarche méthodologique proposée pour assurer la prestation d'Audit de la sécurité des systèmes d'information et tests d'intrusion et garantir la pertinence des services attendus; avec indication des moyens requis pour l'exécution des travaux.
- Les attestations de références du soumissionnaire en matière de réalisation de la prestation d'Audit de la sécurité des systèmes d'information et tests d'intrusion.
- Le délai prévisionnel de réalisation de la mission des tests d'intrusion externes, internes et applicatifs.
- Le délai prévisionnel de réalisation de la mission d'Audit de l'architecture réseau & sécurité SI.
- La composition de l'équipe appelée à intervenir, en précisant les noms et prénoms, les profils et les qualifications professionnelles et les certifications /produits s'il y a lieu des experts,
- Toute la documentation technique des équipements et des logiciels objet du présent appel d'offres nécessaire à l'évaluation de l'offre.
- Les CV complets (avec diplômes & certificats) de l'ensemble des experts et consultants intervenants dans ce projet

5.3.4 Offre Financière

L'offre financière devra être détaillée et conforme au bordereau de prix en annexe II.

L'offre de prix sera ferme et non révisable.

L'entreprise établira un acte d'engagement conformément au modèle joint en annexe III. Par ailleurs, le soumissionnaire pourra joindre à son offre des informations et commentaires qu'il estimera souhaitables pour aider dans leur jugement, les instances chargées de l'appréciation des offres des soumissionnaires.

5.4 Envoi ou dépôt des propositions

Les plis sont, au choix des concurrents :

- Soit déposés, contre décharge à l'adresse indiquée au point 4.2 ci-dessus ;
- Soit envoyés, par courrier recommandé avec accusé de réception, à l'adresse indiquée au point 4.2 ci-dessus.

5.5 Examen des offres

5.5.1 L'examen des offres

L'examen des offres sera effectué par une commission désignée à cet effet par VIVALIS SALAF. Les membres de cette commission sont tenus au secret professionnel pour tout ce qui concerne les éléments portés à leur connaissance.

La meilleure offre sera choisie en tenant compte notamment :

- De sa capacité à répondre aux stipulations du présent cahier des charges en analysant :
 - La démarche méthodologique, la couverture du besoin et l'organisation du projet
 - La qualité et l'expérience des experts proposés
 - Les références dans la réalisation de projets similaires
 - Délai de réalisation des services
- Du montant de l'offre de prix.

5.5.2 La procédure de jugement des offres

La procédure de jugement des offres par la commission s'établit comme suit :

PHASE 1 : Analyse préliminaire des offres

Cette analyse tend à s'assurer de la conformité des propositions par rapport aux stipulations du cahier des charges, notamment les pièces du dossier administratif et technique ainsi que celles de l'offre technique. Elle se matérialise par l'arrêt de la liste des concurrents admissibles.

PHASE 2 : Evaluation des offres techniques.

Seules les offres des concurrents retenus à l'issue de la phase 1 feront l'objet d'un examen par une commission désignée à cet effet par VIVALIS SALAF.

L'offre technique sera notée sur 100 points.

Il est à noter que les candidats ayant obtenu une note inférieure à 70 points dans l'offre technique seront éliminés avant même l'ouverture des plis financiers.

Critères d'évaluation :

CHAMPS	NOTE
Couverture fonctionnelle des besoins	30 points
La qualité et l'expérience des experts proposés	30 points
Les références du soumissionnaire	20 points
Démarche & délais de réalisation des services	20 points

Exigences relatives à l'évaluation des offres

Pour chaque critère d'évaluation, un seuil minimal de 50 % de la note maximale attribuable est requis. Toute offre obtenant une note inférieure à 50 % sur l'un des critères d'évaluation sera considérée comme non conforme et, par conséquent, éliminée du processus de sélection.

PHASE 3 : Evaluation technico-financière

Après élimination des offres non retenues à l'issue de la phase 2, il sera donné à chaque offre une valeur

« Ni » qui est égale à :

$$Ni = (60 \cdot Ti + 40 \cdot Fi) / 100 ;$$

$$Fi = (Po / Pi) \cdot 100.$$

Ti : note technique obtenue par le soumissionnaire,

Po : prix offert par le soumissionnaire le moins disant,

Pi : prix offert par le soumissionnaire.

PHASE 4 : Evaluation générale et adjudication

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

VIVALIS SALAF se réserve l'entièvre liberté dans le choix des propositions et pourra ne donner suite à aucune des propositions présentées, sans être tenue de faire connaître les motifs de sa décision.

5.5.3 Coût de l'appel d'offres

Le soumissionnaire supportera tous les frais afférents à la présentation de son offre et VIVALIS SALAF ne sera en aucun cas responsable de ces coûts de quelque façon que se déroule le processus de l'appel d'offres et quel qu'en soit le résultat.

5.5.4 Demande de renseignement

Les entreprises qui désirent obtenir des éclaircissements sur les spécifications du cahier des charges du présent appel d'offres pourront notifier leur demande à VIVALIS SALAF par écrit sous pli envoyé par la poste ou déposé à l'adresse indiquée au point 4.2 ou messagerie électronique à l'adresse suivante : appeloffres@vivalis.ma

5.5.5 Modifications au cahier des charges

VIVALIS SALAF peut à tout moment avant la date limite de remise des offres, et pour quelque motif que ce soit, à son initiative ou en réponse à une demande d'éclaircissement formulée par un soumissionnaire, modifier par amendement certaines clauses du présent cahier des charges.

La modification sera notifiée par écrit à tous les soumissionnaires participant à l'appel d'offres.

Pour donner aux soumissionnaires les délais nécessaires à la prise en considération de ladite modification dans la préparation, le cas échéant, de leurs nouvelles offres, VIVALIS SALAF a toute latitude de reporter la date limite de remise des offres et aviser les soumissionnaires de ce report.

5.5.6 Modification des propositions

La commission peut, avant d'émettre son avis entendre les soumissionnaires afin d'obtenir tout éclaircissement et explication sur leur proposition. Elle peut éventuellement demander à tous ou à certains soumissionnaires d'apporter certaines modifications à leur proposition.

5.5.7 Durée des engagements

Les Entreprises seront liées par leurs offres pendant soixante (60) jours calendaires à partir de la date limite de remise des offres.

5.5.8 Pénalité de retard

Le délai de livraison convenu avec l'adjudicataire, du présent appel d'offres, débutera à partir de la notification écrite faite par VIVALIS SALAF à ladite Entreprise. Cette dernière aura l'obligation de respecter le délai faute de quoi une pénalité de 0.25% du montant total de l'adjudication, par jour de retard sera appliquée sans toutefois excéder 10%. Au-delà, l'adjudication du présent appel d'offres sera annulé de plein

droit par VIVALIS SALAF. Cette résiliation n'exonère pas l'entreprise du paiement de dommages et intérêts, outre la restitution des sommes payées pour les livraisons et prestations non encore exécutées.

ANNEXES

Annexe 1 : Modèle de déclaration sur l'honneur

Annexe 2 : Bordereau de prix

Annexe 3 : Modèle d'acte d'engagement

Annexe 1

MODELE DE DECLARATION SUR L'HONNEUR

Je soussigné

- Nom, Prénom
- Qualité.....
- Agissant au nom et pour le compte de (raison sociale de l'Entreprise)
- Inscrite au registre de commerce de
- Sous le N°.....
- Affiliée à la CAISSE NATIONALE DE SECURITE SOCIALE sous le °..... et à la TVA sous le N°.....
- Titulaire du compte (bancaire).....(celui de la société).
- Faisant élection de domicile à.....
- En vertu des pouvoirs qui me sont conférés par (décision du conseil d'administration, délégation, etc...)

Déclare

- Appartenir à l'une des professions dont relèvent les prestations relatives à l'objet de la consultation de VIVALIS SALAF.
- Que je ne représente pas plus d'un concurrent dans le présent appel d'offres.
- Que les risques découlant de mon activité professionnelle sont couverts par une police d'assurance dans les limites et conditions prescrites par le cahier des prescriptions spéciales de l'appel d'offres.
- Que je ne suis pas en liquidation judiciaire, ni en redressement judiciaire.
- Que je suis en situation fiscale régulière vis-à-vis de la trésorerie marocaine par ce qu'ayant acquitté les sommes exigibles.

Je certifie sur l'honneur l'exactitude des renseignements ci-dessus.

Fait à..... Le

(Signature et cachet du soumissionnaire)

Annexe 2

Rg	Description	Nbr de JH (*)	Prix Unitaire HT	Prix Total HT
1	Tests d'intrusion externes			
1.1	Boite noire			
1.2	Boite grise			
2	Tests d'intrusion internes			
2.1	Boite noire			
2.2	Boite grise			
2.3	Boite blanche			
3	Tests Applicatifs			
4	Audit d'architecture			
Total HT				

(*) Nbr de jour à détailler en Chef de projet, Expert, Consultant

Annexe 3

MODELE D'ACTE D'ENGAGEMENT

Je soussigné, (Nom, Prénom, Qualité) Agissant au nom et pour le compte de (raison sociale de l'Entreprise), inscrite au registre de commerce de sous le N°....., affiliée à la CAISSE NATIONALE DE SECURITE SOCIALE sous le N°..... et à la TVA sous le N°.....

En vertu des pouvoirs qui me sont conférés, faisant élection de domicile à

.....
.....

Après avoir pris connaissance de toutes les pièces du projet et du cahier des charges concernant l'audit de la sécurité des systèmes d'information et tests d'intrusion faisant l'objet de la consultation du

.....

Après avoir apprécié à mon point de vue et sous ma seule responsabilité, la nature, l'importance, les conditions et difficultés d'exécution des travaux pour avoir examiné, en totalité et en détail, les pièces du dossier,

Remets, en revêtu de ma signature, un bordereau des prix établi conformément aux clauses figurant au dossier.

Me soumets et m'engage à exécuter lesdits travaux conformément au Cahier des Charges moyennant le prix que j'ai établis moi-même, lequel prix fait ressortir à la somme TOUTES TAXES COMPRISSES de : (montant en chiffres et en lettres)

.....

Le montant du détail estimatif

VIVALIS se libérera des sommes dues par elle en faisant donner crédit au compte bancaire ouvert au nom de....., à sous le N°.....

FAIT A..... LE

(Signature et cachet du soumissionnaire)