Termes de référence

ARTICLE 1 : MODE DE PASSATION

La présente consultation sera effectuée dans le cadre de la procédure du bon de commande par voie électronique en application des dispositions :

- De la Section IV du décret n°2-22-431 du 15 chaabane 1444 (8 mars 2023) relatif aux marchés publics ;
- Du Chapitre VIII de l'Arrêté du Ministre délégué auprès de la Ministre de l'Economie et des Finance, chargé du budget n°1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatives aux marchés publics.

ARTICLE 2 : OBJET

Les présents termes de référence ont pour objet de définir les modalités et les conditions de réalisation d'une mission d'audit technique de sécurité du nouveau portail web de l'ONICL, préalablement à sa mise en ligne, conformément aux exigences de la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI), aux dispositions de la loi n° 05-20 relative à la cybersécurité ainsi qu'aux bonnes pratiques en la matière, telles que désignées à l'article 18 ci-dessous.

ARTICLE 3 : CONTEXTE ET OBJECTIFS DE LA MISSION

L'ONICL souhaite réaliser un audit technique de sécurité de son nouveau Portail web avant sa publication conformément aux préconisations de la DNSSI et des bonnes pratiques en la matière.

Les principaux objectifs de cette mission d'audit sont déclinés comme suit :

- ✓ Disposer d'une vision globale et objective du niveau de sécurité du Portail web par rapport aux Directives Nationales de la Sécurité des SI et éventuellement aux référentiels internationaux en la matière ;
- ✓ Auditer la sécurité technique du portail web conformément aux points de contrôle de la Directive Nationale de la Sécurité des Systèmes d'Information ;
- ✓ Dresser un registre des vulnérabilités et d'un plan de remédiation priorisé
- ✓ Elaborer un plan d'action pour se conformer à la loi 05-20 relative à la cybersécurité et la Directive Nationale de la Sécurité des Systèmes d'Information ;

ARTICLE 4 : CERTIFICATS ET ATTESTATIONS A DEPOSER

Chaque concurrent souhaitant participer à la présente consultation est tenu de déposer, au plus tard le **04 Décembre 2026 à 11 h 00**, au bureau d'ordre du siège de l'Office National Interprofessionnel des Céréales et des Légumineuses (ONICL), sis au 3, avenue Moulay El Hassan à Rabat, une enveloppe scellée portant le numéro de l'avis d'achat ainsi que la dénomination sociale du concurrent et contenant les documents suivants :

- **Document (en cours de validité) attestant que le soumissionnaire est qualifié PASSI par la DGSSI dans les domaines suivants :**
  - Audit de configuration ;
  - Tests d'intrusions ;
  - Audit du code source.
- **Pour le Chef de Projet (Expert en sécurité SI), Un certificat parmi la liste ci après :**
  - CERTIFICA CISA
  - CERTIFICAT ISO 27001 :2022 Leader Implementer
  - CERTIFICAT ISO 27001 :2022 Lead Auditor
- **Pour le Consultant spécialiste en test d'intrusion, en plus de l'Attestation PASSI en cours de validité dans le domaine « Test d'intrusion » (obligatoire), Deux certificats parmi la liste ci-après :**
  - CEH (Certified Ethical Hacker)

- OSCP (Offensive Security Certified Professional)
- CPTP (Certified Penetration Testing Professional)
- CNFE (Certified Network Forensics Examiner)
- OSWA (offensive security web assessor)
- GIAC Web Application Penetration Tester (GWAPT) ;
- WPTX (Web application Penetration Tester eXtreme)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN).

- **Pour le Consultant spécialiste en Audit sécurité applicative, en plus de l'Attestation PASSI en cours de validité dans le domaine « audit sécurité applicative » (obligatoire), Deux certificats parmi la liste ci-après :**
  - GIAC Web Application Penetration Tester (GWAPT) ;
  - CWASP: Certificat Professionnel en Sécurité des Applications Web ;
  - WPTX (Web application Penetration Tester eXtreme) ;

- **Pour le Consultant spécialiste dans l'audit des configurations, en plus de l'Attestation PASSI en cours de validité dans le domaine « audit des configurations » (obligatoire), un certificat parmi la liste ci-après :**
  - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) ;
  - GIAC Enterprise Vulnerability Assessor Certification (GEVA) ;

Toute offre non accompagnée du dépôt préalable de l'ensemble des documents susmentionnés, dans les conditions et délais précités, sera écartée.

ARTICLE 5 : OBLIGATIONS DU PRESTATAIRE

Le prestataire s'engage à :

- ✓ Respecter les lois et les règlements en usage au Maroc ;
- ✓ Assumer la responsabilité de ses prestations en respectant les usages et les coutumes de la profession, les dispositions de la loi, de la jurisprudence ainsi que les conséquences dommageables que pourraient générer les défauts de l'exécution de ses prestations ;
- ✓ Respecter tous ses engagements par l'accomplissement de la mission qui lui est confiée et assurer une très haute qualité de service ;
- ✓ Respecter le secret professionnel concernant toutes les informations et tous les documents dont il aura pris connaissance dans le cadre de cette mission. Cette obligation est valable, également, pour ses collaborateurs ;
- ✓ Faire intervenir les cadres proposés, en affectant à ce projet une équipe pluridisciplinaire de haut niveau, ayant une expérience confirmée dans des réalisations similaires.
- ✓ Enfin, le prestataire, du seul fait de l'attribution du bon de commande, reconnaît avoir reçu de l'ONICL toutes les indications générales qui lui sont nécessaires pour l'exécution du bon de commande qui en découlera ;
- ✓ Les intervenants agréés par le maître d'ouvrage au début de la mission ne peuvent être remplacés par de nouveaux intervenants qu'après accord de celui-ci.
- ✓ Si pour des raisons indépendantes de la volonté du prestataire, il s'avère nécessaire de remplacer un ou plusieurs intervenants, ledit titulaire est tenu d'engager, après avis de l'ONICL, des personnes de qualification égale ou supérieure.
- ✓ L'ONICL a le droit d'exiger au prestataire le changement de ses intervenants pour incapacité professionnelle ou défaut de probité.

A cet effet, il devra sur demande de l'ONICL, engager dans un délai de dix (10) jours au maximum, des remplaçants dont la qualification et l'expérience seront soumises à l'approbation du maître d'ouvrage, étant précisé qu'aucune indemnité ne peut lui être accordée au cas où des coûts supplémentaires seraient occasionnés par le retrait ou le remplacement des collaborateurs.

EXIGENCES DE CONFIDENTIALITE :

Le prestataire aura accès à des informations sensibles liées au fonctionnement et à la sécurité du SI de l'ONICL, il est alors tenu de :

- ✓ Ne communiquer aucune information concernant cette mission au public ni à une tierce partie sans le consentement écrit de l'ONICL ;
- ✓ Garantir que le circuit de production des documents liés à la présente mission d'audit est sécurisé (poste de travail, circuit de validation interne, impression des documents, sauvegarde des documents, destruction des documents, etc.) ;
- ✓ Avoir une politique de diffusion de documents selon leur niveau de confidentialité. Tous les documents résultant de l'audit doivent avoir une diffusion restreinte aux personnes concernées par l'audit ;
- ✓ Mettre en place un système sécurisé pour le partage des rapports et livrables avec l'ONICL.
- ✓ Le prestataire garantit formellement le maître d'ouvrage contre toutes les revendications des tiers concernant les brevets d'invention relatifs aux procédés et moyens utilisés, marques de fabrique, de commerce et de service.
- ✓ Il appartient au prestataire le cas échéant, d'obtenir les cessions, licence d'exploitation ou autorisation nécessaires et de supporter la charge des frais et redevances y afférentes.

ARTICLE 6 : JUGEMENT DE L'OFFRE

La commission retiendra l'offre la moins disante parmis les offres jugées conformes.

ARTICLE 7 : DELAI ET LIEU D'EXECUTION

Il est de soixante **(60) jours à compter du jour de remise du bon de commande**.
La livraison s'effectuera au siège central de l'ONICL à l'adresse suivante : **3, Avenue Moulay Hassan - Rabat.**

ARTICLE 8 : PENALITE DE RETARD

À défaut d'avoir terminé la livraison dans le délai prescrit, il sera appliqué au fournisseur une pénalité par jour calendaire de retard d'un pour mille (l%o) du montant initial du bon de commande.

Ces pénalités seront appliquées de plein droit et sans mise en demeure sur toutes les sommes dues au prestataire.

L'application de ces pénalités ne libère en rien le prestataire de l'ensemble des autres obligations et responsabilités qu'il aura souscrites au titre du bon de commande qui sera issu de la présente consultation.

Toutefois, le montant cumulé de ces pénalités est plafonné à 10% du montant initial du bon de commande. Lorsque le plafond des pénalités est atteint, l'ONICL est en plein droit de résilier le bon de commande après mise en demeure préalable.

ARTICLE 9 : RECEPTION

La réception sera prononcée au terme de la mission. Elle concerne la validation des livrables et des prestations fournies et sera sanctionnée par un procès-verbal de réception.

La réception sera prononcée par une commission désignée à cet effet par l'ONICL, qui dressera un procès-verbal de réception.

ARTICLE 10 : ETABLISSEMENT DES PRIX

Les prix comprennent tous les droits, taxes, frais généraux et d'une façon générale toutes les dépenses qui sont la conséquence nécessaire et directe de l'exécution du bon de commande.
Les prix seront établis en dirhams. Le fournisseur est réputé connaître et avoir examiné les conditions économiques prévalant ou pouvant prévaloir pendant la durée de l'exécution du bon de commande issu de la présente consultation.

ARTICLE 11 : NATURE DES PRIX

Le bon de commande, issu de la présente consultation, est à prix unitaire.

ARTICLE 12 : MODALITES DE PAIEMENT

Les sommes dues au fournisseur, en exécution du bon de commande issu de la présente consultation, seront versées au compte du titulaire sur production d'une facture, appuyé du procès verbal de réception, libellée en dirhams, en 3 exemplaires dûment signés respectant la réglementation fiscale et commerciale, mentionnant la TVA et rappelant l'intitulé exact du compte bancaire après déduction des pénalités, le cas échéant.

ARTICLE 13 : ASSURANCES - RESPONSABILITÉ

Le prestataire est réputé souscrire des polices d'assurance inhérents aux risques liés à l'exécution du bon de commande.

ARTICLE 14 : RESILIATION

En cas d'inexécution partielle ou totale des obligations du fournisseur et sauf cas de force majeure, après mise en demeure adressée au prestataire par lettre recommandée avec accusé de réception et demeurée sans effet, l'ONICL aura la faculté de notifier au prestatire la résiliation de plein droit du bon de commande sans qu'il soit besoin d'aucune autre formalité.

L'exercice de cette faculté de résiliation ne dispense pas l'entrepreneur de remplir les obligations contractées jusqu'à la date de prise d'effet de la résiliation.

Toutefois, le bon de commande issu de la présente consultation prendra fin immédiatement et sans dommages ni intérêts :

- si le fournisseur est en redressement ou en liquidation judiciaire ;
- si le fournisseur devient insolvable ;
- ou si le fournisseur effectue le transfert de tout ou d'une partie substantielle de ses actifs en faveur de ses créanciers ou tiers.

ARTICLE 15 : CAS DE FORCE MARJEURE

Il n'y a lieu à aucun dommages-intérêts, lorsque le fournisseur justifie que l'exécution ou le retard proviennent d'une cause qui ne peut lui être imputée, telle que la force majeure.

ARTICLE 16 : LITIGES

Tous les litiges et toutes les contestations qui surviendraient entre l'ONICL et le fournisseur à l'occasion de l'exécution du bon de commande issu de la présente consultation relèveront du tribunal compétent de Rabat.

ARTICLE 17 : DONNEES PERSONNELLES

1- Droits des personnes physiques concernées

Par le fait de soumissionner, le concurrent consent à ce que les données personnelles, communiquées dans son dossier, soient traitées par l'ONICL pour la gestion administrative, comptable et financière des consultations. L'ONICL a pris plusieurs dispositions pour que ce traitement soit effectué conformément à la loi n°09-08. Il garantit aux personnes concernées un droit d'accès, de rectification et d'opposition, pour des motifs légitimes, sur leurs données personnelles en adressant une demande écrite au siège de l'ONICL à Rabat. Ce traitement a fait l'objet d'une demande d'autorisation auprès de la CNDP sous le numéro A-10/2017.

2- Obligations de prestataire

Le fournisseur est amené dans le cadre de la présente prestation à prendre connaissance de données à caractère personnels, il doit en garantir la sécurité et la confidentialité. A cet effet, il s'engage à :

- Empêcher que les données ne soient déformées, endommagées et empêcher toute utilisation détournée, malveillante ou frauduleuse et tout accès qui ne serait pas préalablement autorisé par l'ONICL ;
- Ne traiter les données que dans le cadre des instructions et de l'autorisation reçues de l'ONICL ;
- Procéder, en fin du bon de commande, à la destruction des données, fichiers informatisés ou manuels, figurant sur tout support.

ARTICLE 18 : SPECIFICATIONS TECHNIQUE ET LIVRABLES A FOURNIR

❖ PHASE 1 : CADRAGE ET GESTION DE PROJET

Dans le cadre de cette phase de cadrage, le prestataire devra :

- Tenir des réunions (prise de contact et lancement du projet) et en établir les PV qui devront être validés par les deux parties ;
- Définir et faire valider le périmètre de l'audit ;
- Présenter les méthodologies détaillées ;
- Collecter la documentation technique ainsi que les informations relatives à l'audit et définir les autres documents à collecter au cours de cette mission ;
- Elaborer la note de cadrage avec un planning détaillant les différentes étapes, avec leurs durées et leurs intervenants respectifs.

➢ LIVRABLES DE L'ETAPE 1 :

- Note de cadrage précisant le périmètre, la méthodologie, les outils envisagés et le Planning détaillé de réalisation mentionnant les intervenants par étape de projet.

❖ PHASE 2 : TESTS D'INTRUSION

Il s'agit de mener des opérations de simulation d'attaques, d'intrusions internes et externes, de cracking de mot de passe, de piratage, de vols d'informations, de fraude, d'accès illicites ou malintentionnés, et de toute autre forme d'attaque envisageable. Ceci dans l'objectif d'apprécier la robustesse du Portail de l'ONICL et sa capacité à préserver l'intégrité de ses données.
Ces tests doivent être menés selon une méthodologie à détailler par le prestataire durant la phase de cadrage et en utilisant les outils nécessaires et conformément à l'éthique et les règles d'art en la matière. Cette méthodologie doit être préalablement validé par l'ONICL.
Les tests intrusifs, qui doivent être menés en dehors des horaires de trafic important, **ne doivent en aucun cas altérer, modifier ou détruire les données du SI de l'ONICL, ni perturber le bon fonctionnement de ce dernier**. Il sera de la responsabilité du prestataire de mettre en garde, prévenir et conseiller l'ONICL de tous les risques encourus lors de la mise en œuvre de ces tests.
Pour les tests d'intrusions externes, ils se dérouleront comme suit :
Etape 1 : (boite noire) : les experts procèderont à ces tests en disposant uniquement des informations publiques. Cette phase de découverte a pour objectif :

- D'obtenir un maximum d'informations sensibles sur les services accessibles et les équipements d'infrastructure associés, en cartographiant la plate-forme internet grâce à différentes techniques ;
- D'identifier des vulnérabilités présentes sur les machines exposant ces services ;
- D'énumérer les exploitations possibles de vulnérabilités trouvées et d'évaluer les risques d'intrusion dans les systèmes ONICL.

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

Etape 2 (boite blanche) : plus de détails seront communiqués sur la configuration au prestataire pour effectuer ce test d'intrusion. L'auditeur devra évaluer la robustesse des mécanismes d'authentification (principes et algorithmes utilisés), de gestion de sessions, de cloisonnement des données, de contrôle de paramètre transmis par l'utilisateur. Il est important de s'assurer qu'un utilisateur standard ne peut élever ses privilèges sans autorisation, afin d'obtenir des informations confidentielles ou d'insérer des données falsifiées.

➢ LIVRABLES DE LA PHASE 2 :

Rapport comprenant les résultats des tests d'intrusion internes et externes avec une indication précise de l'impact des vulnérabilités recensés sur la sécurité SI en matière de les combler.
Ce rapport devra comprendre notamment :

- Cartographie des vulnérabilités recensées avec le niveau d'expertise pour exploiter la vulnérabilité ;
- Cartographie des risques d'intrusion ou de cyberattaques.
- Les mesures à mettre en place pour traiter les risques.

Les mesures à mettre en place pour traiter les risques.

❖ PHASE 3 : AUDIT DE CONFIGURATION

L'objectif est de réaliser une évaluation technique de la configuration afin de s'assurer que les mesures de sécurité déployées respectent les bonnes pratiques en la matière.
L'audit devra porter, selon les éléments disponibles, sur :

- **Les technologies utilisées : système d'exploitation, serveur web, framework, CMS, base de données et bibliothèques ;**
- **L'état de maintenance et de mise à jour des composants ;**

➢ **LIVRABLES DE LA PHASE 3 : RAPPORT COMPRENANT NOTAMMENT :**

- Les procédures de gestion à mettre en place ;
- La liste détaillée des vulnérabilités, classifiées en fonction de leur gravité potentielle (conséquences, facilité d'exploitation...).

❖ PHASE 4 : AUDIT DE SECURITE ET DU CODE SOURCE :

L'objectif est d'évaluer le niveau de sécurité Du portail web de l'ONICL.
Le prestataire doit faire un audit du code source en mettant en avant les recommandations à adopter pour renforcer la sécurité du code source.

Les auditeurs devront au minimum effectuer les tests applicatifs et techniques suivants :

- La qualité du code source, sa structure et sa maintenabilité ;
- Les mécanismes d'authentification et de gestion des sessions ;
- La gestion des habilitations et des droits d'accès ;
- Les risques d'accès non autorisé et d'élévation de privilèges ;
- La gestion des erreurs et des exceptions ;
- Les dépendances externes et les interfaces API ;
- Paramètres non validés : Insertion des caractères dans l'URL afin de vérifier la présence de filtres sur les caractères saisis.
- Violation du contrôle d'accès : Tentative d'accès à des comptes ou à des informations qui lui sont interdits. Ce test permet de vérifier la politique de sécurité implémentée sur l'application.
- Compte cassé et gestion de la session : Tentative de modification des mots de passe, des clés et des cookies de sessions. Ce test permet de vérifier si les droits et les jetons de session sont correctement utilisés.
- Gestion de session (vol de session) : Tentative de création de cookies. Ce test permet de vérifier si le "cookie" de session est une valeur aléatoire, imprédictible.
- Failles Cross Site Scripting (XSS) : Tentative d'utilisation de l'application web pour attaquer, via un script, le navigateur des visiteurs de l'application.
- Buffer Overflow applicatif : Tentative d'injection de quantité de données importante dans une variable Web pour provoquer des comportements inattendus de l'application.
- Injection de commandes (ex : SQL injection) : Tentative d'utilisation de l'application Web pour passer des paramètres aux applications back-office ou au système d'exploitation.
- Conditions d'erreur : Tentative de récupération des informations détaillées du système suite à une mauvaise gestion des conditions d'erreur.
- Directory Traversal/ Forceful Browsing : Tentative de modification des requêtes afin qu'elles ne demandent pas à l'application de lui retourner un fichier mais la branche toute entière.
- Administration à distance : Tentative d'accès aux pages d'administration du portail Web.
- Divulgation d'informations sensibles dans le code client (HTML, JavaScript, VBScript) : Tentative de récupération d'informations sensibles dans les traitements des langages de scripts clients, réalisés sur le navigateur.
- Analyse des fonctionnalités SSL : Tentative de contournement des mécanismes SSL mis en œuvre.

➢ **LIVRABLES DE LA PHASE 4 : RAPPORT D'AUDIT DU CODE SOURCE.**

❖ PHASE 5 : RECOMMANDATIONS

Le prestataire est tenu de proposer des recommandations dans ses différents rapports d'audit et éventuellement les solutions nécessaires pour faire face et pallier aux dysfonctionnements, vulnérabilités et risques relevés lors des missions pour chaque axe d'intervention.

Les anomalies à traiter seront classées selon quatre niveaux :

- **Critique :** risque majeur de compromission, d'exposition importante de données ou d'interruption grave du service ;
- **Élevée :** vulnérabilité ou défaut présentant un impact important et nécessitant une correction prioritaire ;
- **Moyenne :** faiblesse technique ou fonctionnelle ayant un impact modéré ou nécessitant des conditions particulières d'exploitation ;
- **Faible :** anomalie à impact limité ou amélioration recommandée.

➢ **LIVRABLES PHASE 5 :**

- Rapport des recommandations pour la mise à niveau de l'existant ;

  - **N-B : TOUS LES RAPPORTS D'AUDIT DOIVENT RESTER CONFIDENTIELS ET NE DOIVENT ETRE COMMUNIQUE QU'A L'ONICL.**

ARTICLE 19 : BORDEREAUX DES PRIX-DETAIL ESTIMATIF

N° Prix	Désignation	Unité de Compte	Quantité	Prix HT	Prix Total HT
01	La réalisation d'une mission d'audit technique de sécurité du nouveau portail web de l'ONICL, préalablement à sa mise en ligne, conformément aux exigences de la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI), aux dispositions de la loi n° 05-20 relative à la cybersécurité ainsi qu'aux bonnes pratiques en la matière.	F	1		
Total HT					
TVA 20%					
Total TTC					

Chef de la Division des Ressources Humaines et des Affaires Administratives

Signé : Mohamed EL ADDANI

TERMES DE REFERENCES

d'Avis d'achat N°27-2026/ONICL/DRHAA/SAMG

Le Directeur de l'Office National Interprofessionnel des Céréales et des Légumineuses	Signature et cachet du concurrent "Lu et approuvé"
Chef de la Division des Ressources Humaines et des Affaires Administratives Signé : Mohamed EL ADDANI	