25/11/2026 CDI_DRHAA_2026_817

ONICL

AVIS D'ACHAT SUR BON DE COMMANDE N°27-2026/ONICL/DRHAA/SAMG

L'Office National Interprofessionnel des Céréales et des Légumineuses procède à l'achat sur bons de commande des prestations objet du présent avis, en application des dispositions de l'article 91 du décret n° 2-22-431 relatif aux marchés publics.

- Objet de la prestation:

Contrôle et expertise techniques : 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.

- Consistance de la prestation:

N°	Désignation	Caractéristiques et spécifications	Unité de mesure	Quantité	Observations
1	**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.**	❖ **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	Forfait	1	**Dépôt obligatoire des certificats et attestations exigés à l'article 4 des TDR, au siège central de l'ONICL à Rabat, au plus tard le 04 décembre 2026 à 11h00.**

		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.**

- Lieu d'exécution: **Rabat.**
- Délai d'exécution des prestations: **60 jours**.
- Date et heure limites de réception des devis des concurrents: **Le 04 Décembre 2026** à **11 heures 00 min**.
- Date et heure limites de dépôt des certificats et attestations exigés : **Le 04 Décembre 2026** à **11 heures 00 min**.
- Les plis des concurrents sont déposés par voie électronique dans le portail des marchés publics accessible à l'adresse www.marchespublics.gov.ma.
- **Condition de résiliation** : En cas d'inexécution partielle ou totale des prestations objet du bon de commande ou en cas de dépassement du délai d'exécution indiqué ci-dessus, l'ONICL aura la faculté de notifier au prestataire la résiliation de plein droit du bon de commande sans qu'il soit besoin d'aucune autre formalité.

Chef de la Division des Ressources Humaines et des Affaires Administratives

Signé : Mohamed EL ADDANI