



**CAHIER DE PRESCRIPTIONS SPECIALES
RELATIF À L'APPEL D'OFFRES OUVERT
SUR OFFRES DE PRIX N°62/2025**

**OBJET : AUDIT DE SECURITE DU SYSTEME D'INFORMATION DU LABORATOIRE
PUBLIC D'ESSAIS ET D'ETUDES - EN LOT UNIQUE**

Etabli en application de l'alinéa 1 paragraphe 1 de l'article 21 du règlement des achats du LPEE RA/980/1, version 02 du 01 Juin 2025 fixant les conditions et les formes dans lesquelles sont passés les marchés pour le compte du Laboratoire Public d'Essais et d'Eudes ainsi que certaines règles relatives à leur gestion et à leur contrôle tel qu'il est publié sur le site www.lpee.ma.

Date limite de dépôt des plis : 07/10/2025 à 10 H 00



SOMMAIRE

Sommaire	2
Chapitre premier : Cahier des Clauses administratives et financières	6
Article 1: Objet du marché	6
Article 2: Présentation du maître d'ouvrage	6
Article 3: Consistance des prestations de services.....	6
Article 4: Documents constitutifs du marché.....	6
Article 5: Pièces contractuelles postérieures à la conclusion du marché	6
Article 6: Référence aux textes généraux et spéciaux applicables au marché.....	7
Article 7: Validité et date de notification de l'approbation du marché	7
Article 8: Pièces mises à la disposition du prestataire de services.....	7
Article 9: Election du domicile du prestataire de services	7
Article 10: Nantissement	8
Article 11: Sous-traitance	8
Article 12: Durée du marché	8
Article 13: Délai d'exécution	9
Article 14: Nature des prix.....	9
Article 15: Caractère des prix	9
Article 16: Cautionnement provisoire et cautionnement définitif.....	10
Article 17: Retenue de garantie.....	10
Article 18: Assurances – Responsabilité	10
Article 19: Propriété industrielle, commerciale ou intellectuelle	11
Article 20: Obligations de discrétion	11
Article 21: Délai de garantie	11
Article 22: Modalités de règlement.....	11
Article 23: Réceptions provisoires et définitive.....	12
Article 24: Pénalités pour retard	12

Article 25: Droits de timbre et d'enregistrement.....	12
Article 26: Lutte contre la fraude et la corruption	13
Article 27: Résiliation du marché.....	13
Article 28: Règlement des différends et litiges	13
Chapitre II : Cahier des prescriptions techniques	14
Article 29: LOT 1 : AUDIT DE SECURITE DU SYSTEME D'INFORMATION DU LABORATOIRE PUBLIC D'ESSAIS ET D'ETUDES	14
Article 30: Description du SI du LPEE.....	15
Article 31: Architecture générale	15
Article 32: Composantes principales	15
Article 33: Propriété des études.....	16
Article 34: Livrables	16
Article 35: Informations.....	16
Article 36: Engagements.....	16
Article 37: PERIMETRE DU PROJET	17
Article 38: Définition des prix.....	26
Bordereau des prix – Détail estimatif	27
DERNIERE PAGE.....	28



OBJET : AUDIT DE SECURITE DU SYSTEME D'INFORMATION DU LABORATOIRE PUBLIC D'ESSAIS ET D'ETUDES - EN LOT UNIQUE

ENTRE

Le Laboratoire Public d'Essais et D'Etudes (L.P.E.E), société anonyme au capital de 247 702 400,00 Dhs (Deux Cent Quarante Sept Millions Sept Cent Deux Mille Quatre Cent Dirhams), inscrit au registre de commerce de Casablanca sous le N° 32131, affilié à la Caisse Nationale de sécurité sous le n° 1066308, ICE N° 001527537000028, représenté par **Monsieur Hammou Bensaadout**, Directeur Général dudit laboratoire en vertu des pouvoirs qui lui sont conférés, faisant élection de domicile à Casablanca, 25 Rue d'Azilal.

Désigné ci-après par le terme « **Maître d'ouvrage** » ou « **LPEE** »,

D'UNE PART

ET

Cas d'une personne physique

..... (Raison sociale et forme juridique),

M..... qualité.....

Agissant en son nom et pour son propre compte.

Au capital social Patente n°

Registre de commerce de Sous le n°

Affilié à la CNSS sous n°

ICE n°

Faisant élection de domicile au

Compte bancaire RIB (24 positions).....

Ouvert auprès de.....

Désigné ci-après par le terme « **Prestataire de services** » ou « **Titulaire** »,

D'AUTRE PART

Cas d'une personne morale

..... (Raison sociale et forme juridique),

Représenté par M. qualité..... en

vertu des pouvoirs qui lui sont conférés.

Au capital social Patente n°

Registre de commerce de Sous le n°

Affilié à la CNSS sous n°

ICE n°

Faisant élection de domicile au

Compte bancaire RIB (24 positions).....

Ouvert auprès de.....

Désigné ci-après par le terme « **Prestataire de services** » ou « **Titulaire** »,

D'AUTRE PART



Cas d'un groupement

Les membres du groupement soussignés constitués aux termes de la convention(les références de la convention)..... :

Membre 1 :

..... (*Raison sociale et forme juridique*),

Représenté par M. qualité en vertu des pouvoirs qui lui sont conférés.

Au capital social Patente n°

Registre de commerce de Sous le n°

Affilié à la CNSS sous n°

ICE n°

Faisant élection de domicile au

Compte bancaire RIB (*24 positions*)

Ouvert auprès de.....

Membre 2 :

(Servir les renseignements le concernant)

.....
.....

Membre n :

(Servir les renseignements le concernant)

.....
.....

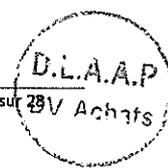
Nous nous obligeons (conjointement ou solidairement, selon la nature du groupement) ayant M..... (Prénom, nom et qualité) en tant que mandataire du groupement et coordonnateur de l'exécution des prestations, ayant un compte bancaire commun sous n° (RIB sur 24 positions)

Ouvert auprès de

Désigné ci-après par le terme « Prestataire de services » ou « Titulaire »,

D'AUTRE PART

IL A ETE ARRETE ET CONVENU CE QUI SUIT



Article 1: **Objet du marché**

Le présent marché a pour objet **audit de sécurité du système d'information du laboratoire public d'essais et d'études** pour le compte du Laboratoire Public d'Essais et d'Etudes (LPEE) en un (01) lot unique, dont les détails figurent dans le cahier des prescriptions techniques et les quantités sont spécifiées dans le bordereau des prix-détail estimatif.

Article 2: **Présentation du maître d'ouvrage**

Autorité compétente : Le Directeur Général du LPEE.

Maître d'ouvrage : Le Laboratoire Public d'Essais et d'Etudes représenté par son Directeur Général.

La Direction de la Logistique, des Achats, des Approvisionnements et de la gestion du Patrimoine du LPEE (DLAAP) est chargée de la gestion administrative du présent marché.

La Direction d'organisation et des systèmes d'information (DOSI) est chargée, sur le plan technique, du suivi de l'exécution du présent marché.

Article 3: **Consistance des prestations de services**

Les prestations de services à réaliser au titre du présent marché font l'objet **audit de sécurité du système d'information du laboratoire public d'essais et d'études en un lot unique**.

Article 4: **Documents constitutifs du marché**

Les documents constitutifs du marché sont ceux énumérés ci-après :

- a) Le bordereau des prix-détail estimatif ;
- b) L'acte d'engagement ;
- c) Le cahier des prescriptions spéciales (CPS) ;
- d) Règlement de consultation (RC) ;
- e) L'offre technique ;
- f) La déclaration sur l'honneur ;
- g) Le cahier des clauses générales applicables aux marchés de services exécutées pour le compte du LPEE (CCGS).

En cas de discordance ou de contradiction entre les documents constitutifs du marché, ceux-ci prévalent dans l'ordre où ils sont énumérés ci-dessus.

Article 5: **Pièces contractuelles postérieures à la conclusion du marché**

Les pièces contractuelles postérieures à la conclusion du marché comprennent :

- Les ordres de service ;
- Les avenants éventuels ;
- La décision prévue à l'article 33 du CCGS, relative à la résiliation du marché.

Les avenants et la décision susvisés sont soumis à l'approbation de l'autorité compétente.

Article 6: Référence aux textes généraux et spéciaux applicables au marché

Les parties contractantes du marché sont soumises aux dispositions des textes suivants :

- La loi n°69-00 relative au contrôle financier de l'état sur les entreprises publiques et autres organismes, promulguée par le Dahir n°1-03-195 du 16 ramadan 1424 (11 novembre 2003) ;
- La loi n 112.13 du 29 rabii II 1436 (19 février 2015) relative au nantissement des marchés publics ;
- Dahir n°1-00-91 du 15 février 2000 portant promulgation de la loi n °17-97 sur la protection de la propriété intellectuelle ;
- Le Règlement relatif aux conditions et formes de passation des marchés du LPEE RA/980/1, version 02 du 01 Juin 2025 ;
- Le Cahier des Clauses Générales applicables aux marchés de services passés pour le compte du LPEE (CCG/980/01) ;
- Tous les textes réglementaires rendus applicables au Maroc à la date de signature du marché et qui sont en rapport avec l'objet du présent marché.

Le prestataire de services devra se procurer ces documents, s'il ne les possède pas, et ne pourra en aucun cas exciper de l'ignorance de ceux-ci, et se dérober aux obligations qui y sont contenues.

Article 7: Validité et date de notification de l'approbation du marché

Le présent marché ne sera valable et définitif qu'après son approbation par l'autorité compétente.

L'approbation du marché doit intervenir avant tout commencement d'exécution. Cette approbation sera notifiée dans un délai maximum de soixante-quinze (75) jours à compter de la date d'ouverture des plis.

L'approbation des marchés ne doit être apposée par l'autorité compétente qu'après l'expiration d'un délai d'attente d'une durée de quinze (15) jours à compter du jour suivant la date d'achèvement des travaux de la commission d'ouverture des plis.

Article 8: Pièces mises à la disposition du prestataire de services

Aussitôt après la notification de l'approbation du marché, le maître d'ouvrage remet gratuitement au prestataire de services, contre décharge, les documents constitutifs du marché en l'occurrence les pièces expressément désignées à l'article 4 du présent marché à l'exception du cahier des clauses générales applicables aux marchés de services, qui peut être téléchargé sur le site du LPEE : www.lpee.ma.

Le maître d'ouvrage ne peut délivrer ces documents qu'après constitution du cautionnement définitif.

Article 9: Election du domicile du prestataire de services

Toutes les correspondances relatives au présent marché sont valablement adressées au domicile du prestataire de services sis.....



En cas de changement de domicile, le prestataire de services est tenu d'en aviser le maître d'ouvrage, par lettre recommandée avec accusé de réception, dans un délai de quinze (15) jours suivant la date d'intervention de ce changement.

Article 10: Nantissement

Dans l'éventualité d'une affectation en nantissement du présent marché, il est stipulé que :

- 1) la liquidation des sommes dues par, le maître d'ouvrage, en exécution du présent marché et leurs paiements seront opérés par les soins de Monsieur le Directeur Général du LPEE, seul qualifié pour recevoir les significations des créanciers du titulaire du marché ;
- 2) Au cours de l'exécution du marché, les documents cités à l'article 8 de la loi n°112-13 peuvent être requis du maître d'ouvrage, par le titulaire du marché ou le bénéficiaire du nantissement ou de la subrogation, et sont établis sous sa responsabilité ;
- 3) Lesdits documents sont transmis directement à la partie bénéficiaire du nantissement avec communication d'une copie au prestataire de services, dans les conditions prévues par l'article 8 de la loi n° 112-13.

Le maître d'ouvrage délivre sans frais, au prestataire de services, sur sa demande et contre récépissé, un exemplaire spécial du marché portant la mention "exemplaire unique" et destiné à former titre conformément aux dispositions législatives relatives au nantissement des marchés de l'état et des établissements publics tel que modifié et complété, et ce, en application du paragraphe 4 de l'article 11 du CCGS.

Article 11: Sous-traitance

Si le prestataire de services envisage de sous-traiter une partie du marché, il doit requérir l'accord préalable du maître d'ouvrage auquel il est notifié la nature des prestations de services à sous-traiter, la raison ou la dénomination sociale, l'adresse et l'identité des sous-traitants et une copie conforme du contrat de sous-traitance.

Les sous-traitants doivent satisfaire aux conditions requises aux concurrents à l'article 28 du règlement des achats du LPEE.

Le prestataire de services demeure personnellement responsable de toutes les obligations résultant du marché tant envers le maître d'ouvrage que vis-à-vis des ouvriers et des tiers. Le maître d'ouvrage ne se reconnaît aucun lien juridique avec les sous-traitants.

Article 12: Durée du marché

La durée du marché est de **douze (12) mois** et ce, à compter de la date prévue par l'ordre de service prescrivant le commencement de la réalisation de la prestation.

Toutes les prolongations de La durée du marché doivent être concrétisées par voie d'avenants selon les dispositions de l'article 10 CCGS.

Article 13: Délai d'exécution

Le prestataire de services devra exécuter les prestations désignées en objet, prescrites par ordre de service, selon le calendrier suivant :

Phases	Délai d'exécution
Cadrage et structuration du projet	10 jours à partir de la date prévue par l'ordre de service prescrivant le commencement de la prestation.
Audit de sécurité technique	2 mois à partir de la date prévue par l'ordre de service prescrivant le commencement de la prestation.
Audit organisationnel	
Audit de configuration et Architecture	
Feuille de route et plan d'action SSI	
Formation et transfert de compétences	15 jours à partir de la date prévue par l'ordre de service prescrivant le commencement de la prestation.

Le délai de livraison court à partir de la date prévue par l'ordre de service prescrivant le commencement de la prestation.

Article 14: Nature des prix

Le présent marché est à prix unitaires.

Les sommes dues au prestataire de services sont calculées par application des prix unitaires portés au bordereau des prix-détail estimatif, joint au présent cahier des prescriptions spéciales, aux quantités réellement exécutées conformément au marché.

Les prix du marché sont réputés comprendre toutes les dépenses résultant de l'exécution des prestations y compris tous les droits, impôts, taxes, frais généraux, faux frais et assurer au prestataire de services une marge pour bénéfice et risques et d'une façon générale toutes les dépenses qui sont la conséquence nécessaire et directe du travail.

Article 15: Caractère des prix

Le présent marché est passé à prix fermes et non révisables et s'entendent comme suit :

Toutes taxes comprises, rendu au siège du LPEE, sis 25 rue d'Azilal, Casablanca- Maroc.

Toutefois, si le taux de la taxe sur la valeur ajoutée est modifié postérieurement à la date limite de remise des offres, le maître d'ouvrage répercute cette modification sur le prix de règlement.

Article 16: Cautonnement provisoire et cautionnement définitif

Le cautionnement provisoire, **ne comportant aucune date limite**, est fixé à : **Dix-mille (10 000,00)**

Le cautionnement provisoire reste acquis au LPEE, notamment dans les cas suivants :

- Si le soumissionnaire retire son offre ou se désiste pendant le délai de validité des offres ;
- Si l'offre du soumissionnaire ayant présenté l'offre la plus avantageuse est écartée pour les motifs suivants :
 - Ne fournit aucune réponse ;
 - Ne régularise pas les discordances constatées entre les diverses pièces de son dossier administratif, technique et additif ;
 - Ne confirme pas les rectifications des erreurs matérielles relevées ;
 - Fournit des justifications non convaincantes en ce qui concerne le ou les prix unitaires principaux jugés excessifs ou anormalement bas, le cas échéant.
- Dans le cas de la défaillance du groupement quel que soit le membre défaillant et ce, conformément aux dispositions de l'article 136 du règlement des achats du LPEE ;
- Si le titulaire refuse de signer le marché ;
- Si le titulaire ne dépose pas le cautionnement définitif dans les trente (30) jours suivant la notification de l'approbation du marché.

Le cautionnement provisoire ou la caution qui le remplace sera libéré conformément aux dispositions de l'article 26 du règlement des achats du LPEE.

Le montant du cautionnement définitif, **ne comportant aucune date limite**, est fixé à **trois pour cent (3%)** du montant initial du marché. Il doit être constitué dans les trente (30) jours qui suivent la notification de l'approbation du marché. Il reste affecté à la garantie des engagements contractuels de l'attributaire jusqu'à la réception définitive des prestations.

Le cautionnement définitif sera restitué ou la caution qui le remplace est libérée à la suite d'une mainlevée délivrée par le maître d'ouvrage dans un délai maximum de quatre-vingt-dix (90) jours suivant la date de la réception définitive des prestations et sous réserves des dispositions prévues par l'article 16 du CCGS.

Article 17: Retenue de garantie

Aucune retenue de garantie ne sera prélevée au titre du présent marché.

Article 18: Assurances – Responsabilité

Le prestataire de services doit adresser au maître d'ouvrage, avant tout commencement de réalisation des prestations de service, les copies des polices d'assurance qu'il doit souscrire et qui doivent couvrir tous les risques inhérents à la réalisation du marché, et ce, conformément aux dispositions de l'article 20 du CCGS. Il devra contracter dès le début d'exécution du marché, et pendant toute la durée de celui-ci, une assurance couvrant les risques suivants :

- La responsabilité découlant de l'utilisation des véhicules automobiles pour les besoins de l'exécution du marché conformément à la législation et à la réglementation en vigueur ;

- La responsabilité d'accident du travail survenant à ses agents conformément à la législation et à la réglementation en vigueur.

Le maître d'ouvrage ne peut être tenu pour responsable des dommages ou indemnités légales à payer en cas d'accidents survenus aux employés du prestataire de services ou ses sous-traitants.

A ce titre, le prestataire de services garantira le maître d'ouvrage contre toute demande de dommages-intérêts ou indemnités et contre toute réclamation, plainte, poursuite, frais, charge et dépense de toute nature relative à ces accidents.

Article 19: Propriété industrielle, commerciale ou intellectuelle

Le prestataire de services 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 de services 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 20: Obligations de discrétion

Le prestataire de services qui, soit avant la notification du marché, soit au cours de son exécution, a reçu communication, à titre confidentiel, de renseignements, documents ou objets quelconques, est tenu de maintenir confidentielle cette communication. Ces renseignements, documents ou objets quelconques ne peuvent, sans autorisation, être communiqués à d'autres personnes que celles qui ont qualité pour en connaître.

Le maître d'ouvrage s'engage à maintenir confidentielles les informations, signalées comme telles, qu'il aurait pu recevoir du prestataire de services.

Article 21: Délai de garantie

Aucun délai de garantie n'est exigé au titre du présent marché.

Article 22: Modalités de règlement

Pour l'établissement des ordres de paiement, le prestataire de services est tenu de fournir au maître d'ouvrage une facture appuyée par attachements signés et cachetés par le LPEE, et d'une copie de l'ordre de service signé et cacheté par le fournisseur, et doit être établie en trois (03) exemplaires décrivant les fournitures livrées et indiquant les quantités livrées, le montant total à payer ainsi que tous les éléments nécessaires à la détermination de ce montant.

La facture doit être établie et déposée contre accusé de réception, au plus tôt, à la date de fin de réalisation des prestations de services, et au plus tard, le dernier jour du mois de fin de réalisation des prestations de services. La facture doit également porter l'ensemble des mentions obligatoires conformément aux dispositions de l'article 145 du Code Général des Impôts.

Si le prestataire de services n'établit pas et/ou ne dépose pas la facture dans le délai précité, ou que la facture ne respecte pas les mentions obligatoires, toutes les sanctions pour infraction aux délais de paiement que le maître d'ouvrage devra verser au trésor conformément aux dispositions de la loi 69.21 publiée au Bulletin Officiel n°7204 du 15 juin 2023 seront déduites des sommes dues au fournisseur de plein droit et sans mise en demeure préalable.

Le règlement sera effectué sur la base desdits ordres de paiement en application des prix du bordereau des prix – détail estimatif aux quantités réellement livrées. Déduction faite de l'application des pénalités de retard le cas échéant.

Sur ordre du maître d'ouvrage, les sommes dues au prestataire de services seront versées au Compte bancaire RIB (24 positions)..... ouvert auprès de (la banque) à quatre-vingt-dix (90) jours fin du mois de la date de facture.

Article 23: Réceptions provisoires et définitive

A l'achèvement des prestations de services et en application de l'article 49 du CCGS, le maître d'ouvrage s'assure en présence du prestataire de services de la conformité des prestations de services aux spécifications techniques du marché et prononcera, eu égard à l'absence de délai de garantie, la réception provisoire et définitive.

S'il constate que les prestations de services présentent des insuffisances ou des défauts ou ne sont pas conformes aux spécifications du marché, le prestataire de services procédera aux réparations et rectifications nécessaires conformément aux règles de l'art. À défaut, la réception ne sera pas prononcée, et le délai d'exécution ne sera pas prorogé pour autant.

Les opérations sus mentionnées sont sanctionnées par l'établissement d'un procès-verbal de réception provisoire et définitive signé par les membres de la commission de réception désignée à cet effet.

Article 24: Pénalités pour retard

A défaut d'avoir réalisé les prestations de services dans le délai prescrit à l'article 13 du présent marché, il sera appliqué au prestataire de services une pénalité par jour calendaire de retard **d'un pour mille (1‰)** du montant de la tranche considérée du marché modifiée ou complétée éventuellement par les avenants.

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

L'application de ces pénalités ne libère en rien le prestataire de services de l'ensemble des autres obligations et responsabilités qu'il aura souscrites au titre du présent marché.

Toutefois, le montant cumulé de ces pénalités est plafonné à dix pour cent (10%) du montant initial du marché modifié ou complété éventuellement par des avenants, tel que stipulé dans l'article 42 du CCGS.

Lorsque le plafond des pénalités est atteint, l'autorité compétente est en droit de résilier d'office le marché et sans préjudice de l'application des mesures coercitives conformément aux dispositions de l'article 52 du CCGS applicable aux marchés de services.

Article 25: Droits de timbre et d'enregistrement



Conformément à l'article 6 du CCGS applicable aux marchés de services, le prestataire de services doit acquitter les droits auxquels peuvent donner lieu l'enregistrement et timbre du marché, tels qu'ils résultent des lois et règlements en vigueur.

Article 26: Lutte contre la fraude et la corruption

Le prestataire de services ne doit pas recourir par lui-même ou par personne interposée à des actes de corruption, à des manœuvres frauduleuses, et à des pratiques collusoires, à quelque titre que ce soit, dans les différentes procédures de passation, de gestion et d'exécution du marché.

Le prestataire de services ne doit pas faire, par lui-même ou par personne interposée, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion d'un marché et lors des étapes de son exécution.

Les dispositions du présent article s'appliquent à l'ensemble des intervenants dans la réalisation du présent marché.

Article 27: Résiliation du marché

La résiliation du marché peut être prononcée conformément aux dispositions prévues aux articles 27 à 33 CCGS du LPEE applicable aux marchés de services.

La résiliation du marché ne fera pas obstacle à la mise en œuvre de l'action civile ou pénale qui pourrait être intentée au prestataire de services en raison de ses fautes ou infractions.

Si des actes frauduleux, des infractions réitérées aux conditions de travail ou des manquements graves aux engagements pris ont été relevés à la charge du prestataire de services, le maître d'ouvrage, sans préjudice des poursuites judiciaires et des sanctions dont le prestataire de services est passible, peut par décision motivée, après avis de la Commission des Achats, et approbation de l'autorité compétente, l'exclure temporairement ou définitivement de la participation aux marchés du LPEE.

Article 28: Règlement des différends et litiges

Si au cours de la réalisation du marché, des différends et litiges surviennent avec le prestataire de services, les parties s'engagent à régler ceux-ci dans le cadre des stipulations des articles 52, 53 et 54 du CCGS du LPEE applicable aux marchés de services.

Les litiges entre le maître d'ouvrage et le prestataire de services sont soumis aux tribunaux compétents de Casablanca.

Article 29: LOT 1 : AUDIT DE SECURITE DU SYSTEME D'INFORMATION DU LABORATOIRE PUBLIC D'ESSAIS ET D'ETUDES

1) CONTEXTE DE LA MISSION :

Dans le cadre du renforcement de la sécurité du système d'information, et en alignement avec les exigences réglementaires, les normes en vigueur ainsi que la stratégie nationale de cybersécurité, le LPEE prévoit de mener une mission d'audit de la sécurité des systèmes d'information (SI). Cette initiative vise à évaluer en profondeur les différentes composantes des SI afin d'atteindre un niveau de sécurité conforme aux exigences réglementaire et normatives.

L'audit portera sur plusieurs volets complémentaires : un audit technique, organisationnel, de configuration ainsi que de l'architecture des systèmes d'information. L'ensemble de ces analyses permettra d'identifier les vulnérabilités potentielles, de mesurer les écarts par rapport aux référentiels de sécurité, et de proposer une feuille de route et un plan d'action correctives en matière de cybersécurité pour le LPEE.

2) OBJECTIF DE LA MISSION :

Les objectifs visés par cette mission d'audit sont notamment les suivants :

- Evaluer le niveau de maturité du SI de LPEE en matière de sécurité
- Mettre à l'épreuve l'infrastructure firewall et internet des systèmes d'information ;
- Rechercher et exploiter des vulnérabilités réseau/ système/ applicatives ;
- Mettre en évidence les vulnérabilités que pourrait exploiter un individu malveillant se situant à l'intérieur et/ou l'extérieur du système d'information, sans ou avec des connaissances préalables du réseau et sans accès spécifiques ;
- Faire apparaître les failles et les risques conséquents d'intrusions (tentatives de fraude, accès et manipulation illicites de données, interception de données critiques, Ecoute réseau, Défis d'accès ...), ainsi que celles virales ;
- Réaliser une évaluation technique de la configuration des composants du système d'information afin de s'assurer que les mesures de sécurité déployées respectent les bonnes pratiques en matière de sécurité ;
- Réaliser une évaluation technique de l'architecture : vérifier le schéma d'architecture global, séparation des environnements (développement, test, production), redondance, segmentation, principes de cloisonnement, interconnexions internes et externes, revue des flux critiques ;
- Empêcher la divulgation/modification non autorisée des données ;
- Empêcher les accès non autorisés aux ressources informatiques (infrastructure, réseaux, applications, données) ;
- Evaluer la gouvernance de la sécurité des systèmes d'information ;
- Evaluer la conformité réglementaire et normative ;
- Proposer des solutions pour pallier les risques et dysfonctionnements ;
- Proposer une feuille de route détaillée et un plan d'action de sécurité des systèmes d'information de LPEE ;

Le titulaire assurera la conduite complète de la mission d'audit tout au long de sa durée, et élaborera en collaboration avec le LPEE, les éléments suivants :

- Avant le début des missions opérationnelles de l'audit, le calendrier détaillé de réalisation des différentes phases ;
- La liste des tâches intermédiaires et les modalités de leur suivi ;
- Le tableau de bord qui est remis à LPEE lors de chaque réunion de suivi d'avancement du projet.

3) SUIVI DES PRESTATIONS PAR LE TITULAIRE ET EQUIPE PROPOSEE :

Le titulaire devra constituer une équipe dédiée, composée de profils expérimentés disposant des compétences techniques requises pour la réalisation des prestations décrites dans le cadre du présent appel d'offres. Cette équipe sera chargée de l'exécution opérationnelle du marché.

Par ailleurs, le titulaire devra désigner un interlocuteur unique, agissant en tant que chef du projet, qui assurera le pilotage global, le suivi des travaux, ainsi que la coordination avec les responsables désignés de LPEE, jusqu'à la validation finale des livrables.

Tout changement d'un membre de l'équipe doit être préalablement validé par LPEE. Le nouveau membre doit justifier d'un profil et une expérience au moins équivalents à ceux du membre remplacé.

Article 30: Description du SI du LPEE

Le système d'information de LPEE constitue le socle central de ses activités opérationnelles et stratégiques. Il est composé de plusieurs composantes interconnectées visant à assurer la gestion efficace des activités, la communication interne et externe, ainsi que la gestion des données critiques.

Article 31: Architecture générale

Le SI repose sur une infrastructure informatique combinant des serveurs localisés dans nos datacenters internes, ainsi que des services en cloud pour certaines applications critiques et collaboratives. LPEE utilise principalement une architecture client-serveur avec des accès sécurisés à distance pour les utilisateurs.

Article 32: Composantes principales

Serveurs et équipements réseau : Plusieurs serveurs dédiés hébergent les applications métiers, les bases de données, les services de messagerie, et les systèmes de gestion des ressources humaines et financières. L'infrastructure réseau comprend des commutateurs, et des firewalls.

Applications métiers : Le SI intègre des applications spécifiques, deux sont développées en interne et les autres sont acquises auprès de fournisseurs, couvrant les domaines tels que la gestion commerciale, et les ressources humaines (AGIRH, SAGE1000, GESTCOM, etc).

Sécurité : Le SI dispose de solutions de sécurité comprenant des antivirus, pare-feu, et des mécanismes d'authentification pour l'accès aux ressources sensibles.

Utilisateurs : Le système supporte utilisateurs répartis entre le siège et les sites distants. Les profils d'accès sont différenciés selon les rôles et les besoins métiers.

Gestion des données : Les données sont stockées dans des bases de données relationnelles avec des sauvegardes régulières assurant la résilience et la continuité des activités.

Services web :

Notamment le site web accessible au public, et des application web utilisées en interne.

Ces différentes solutions sont hébergées dans un datacenter interne, comprenant différents serveurs (DNS, WEB, Bases de données, Messagerie, AD, etc.). La majorité des serveurs sont virtualisés.

Des éléments techniques supplémentaires plus détaillés, seront communiqués au titulaire pour cette mission d'audit.

Article 33: Propriété des études

Tous les documents établis dans le cadre du présent audit par le titulaire sont la propriété exclusive de LPEE qui pourra les utiliser sans aucune redevance ni restriction.

Article 34: Livrables

Tous les livrables demandés devront être remis à la fois en version papier et en version électronique exploitable (au format modifiable tel que Word, Excel ou PowerPoint, selon la nature du livrable).

La version électronique devra être structurée, clairement nommée et facilement réutilisable par les équipes de LPEE.

Le prestataire s'assurera que l'ensemble des documents transmis soient complets, lisibles, et conformes aux exigences de qualité.

Article 35: Informations

LPEE mettra, dans la mesure du possible, à la disposition du titulaire tout document, information ou donnée jugés nécessaires pour la mission.

Le titulaire doit s'engager à respecter la confidentialité des données et informations dont il aura eu connaissance lors de l'accomplissement de sa mission.

Article 36: Engagements

Le titulaire sera entièrement responsable de l'évaluation de l'ampleur des travaux à réaliser, en tenant compte des objectifs fixés dans le cadre de la présente mission.

L'ensemble des rapports, livrables et documents produits dans le cadre de la mission seront la propriété exclusive de LPEE. Le titulaire s'engage à ne pas en faire usage ultérieurement sans autorisation écrite préalable de LPEE.

Il devra également garantir la confidentialité absolue de toutes les informations et documents mis à sa disposition dans le cadre de cette mission (Le titulaire devra signer un engagement de confidentialité avant le démarrage de l'exécution des prestations prévues dans le cadre du présent marché).

Les informations et documents jugés utiles pour l'appréciation et la validation des rapports, doivent être communiqués par le titulaire, sous formats papiers et électronique exploitable.



Par ailleurs, le titulaire s'engage à n'utiliser les données collectées que dans le strict cadre de la mission d'audit pour laquelle il a été mandaté, et à exclure tout usage à d'autres fins.

Article 37: PERIMETRE DU PROJET

La mission d'audit portera sur un périmètre couvrant les volets technique, fonctionnel et organisationnel du SI de LPEE :

La mission d'audit s'appliquera à un périmètre couvrant les dimensions **technique, fonctionnelle et organisationnelle** du système d'information du LPEE, et se déroulera sur plusieurs sites, à savoir :

- Le siège du LPEE,
- Deux (2) sites localisés à Casablanca,
- Deux (2) sites régionaux dont le choix sera arrêté en concertation avec le titulaire.
- **Périmètre technique** : Il couvre l'infrastructure matérielle et logicielle du SI, notamment les systèmes, les réseaux, les bases de données, les dispositifs de sécurité, ainsi que les postes de travail.
- **Périmètre fonctionnel** : Il concerne les principales applications supportant les activités de LPEE.
- **Périmètre organisationnel** : Il couvre l'ensemble des processus métiers et activités liés à la gestion, à l'exploitation et à la gouvernance du système d'information.

Description des prestations attendues

Dans le cadre du présent appel d'offres, les prestations à réaliser sont structurées en 6 phases distinctes.

PHASE 1 : Cadrage et structuration du projet

➤ Objectif

Cette étape a pour objectif de s'approprier le contexte technique global, d'identifier et comprendre en détail les infrastructures et applicatifs existants, les des différentes composantes du SI de LPEE, de définir le plan de travail, ainsi que de préparer et cadrer le périmètre de l'étude.

Lors de cette étape, le titulaire devra notamment :

- Visiter les locaux de LPEE en vue de la réalisation des prospections nécessaires.
- Tenir des réunions de prise de contact et lancement du projet.
- Prendre connaissance du contexte organisationnel, technique et environnemental de LPEE.
- Présenter la méthodologie détaillée de déroulement de cette mission
- Collecter la documentation jugée utile pour accomplir cette mission ;
- Elaborer, fournir et présenter le plan de management de projet ;
- Elaborer, fournir et présenter le plan d'assurance qualité ;

➤ Démarche

Au lancement de la mission, Le prestataire organise une réunion de lancement dans les locaux de LPEE au cours de laquelle les principaux interlocuteurs du projet seront représentés :

- Chefs de projet côté prestataire et côté LPEE ;
- Principaux interlocuteurs amenés à être impliqués dans le projet ;

Cette réunion sera l'occasion pour le prestataire de :

- Présenter le contexte du projet et les référentiels considérés
- Présenter la démarche adoptée et le périmètre de la mission
- Identifier les acteurs qui devront être associés au projet
- Présenter le planning d'exécution de la mission.

➤ Livrables

- Support de Lancement
- Plan d'assurance qualité.
- Plan de management du projet.
- Planning de la mission.
- Supports de formation.

PHASE 2 : Audit de sécurité technique

Il s'agit de mener des opérations de simulation d'attaques, d'intrusions internes et externes, 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 de la sécurité de SI de LPEE et sa capacité à préserver la disponibilité, la confidentialité, et l'intégrité de ses données.

Cette opération vise à auditer les éléments suivants :

- Architecture réseau/sécurité.
- Équipements et produits de sécurité (pares-feux, antivirus, ...)
- Systèmes (serveurs Windows/Linux, bases de données, services, ...)
- Solution de sauvegarde.
- Parc applicatif.
- Tests de vulnérabilités ou tests d'intrusion.

Les tests d'intrusion devront être réalisés en dehors des périodes de forte activité, afin de limiter tout impact sur le fonctionnement du SI. En aucun cas, ces tests ne doivent altérer, modifier ou détruire les données, ni perturber la continuité des services. Il incombera au titulaire de prévenir LPEE des risques potentiels liés à la mise en œuvre de ces tests, de formuler les recommandations nécessaires, et de prendre toutes les précautions requises.

Ces tests doivent être menés selon une méthodologie à détailler par le titulaire et en utilisant les outils nécessaires et conformément à l'éthique et les règles d'art en la matière. Cette méthodologie devra faire l'objet d'une validation préalable par LPEE avant tout démarrage des opérations.

Pour la partie web, le titulaire devra réaliser l'ensemble des évaluations techniques nécessaires afin de détecter d'éventuelles vulnérabilités susceptibles d'impacter la sécurité du SI de LPEE.

À l'issue de cette analyse, il devra produire un rapport d'évaluation du niveau de maturité des services web de LPEE, incluant l'identification et la classification des vulnérabilités selon les dernières recommandations de l'OWASP.

Pour les tests d'intrusion, ils se dérouleront sur deux étapes :

Etape 1 : Tests d'intrusion Externes

Les experts du titulaire réaliseront ces tests en se basant uniquement sur les informations accessibles publiquement.

➤ **Objectif**

Cette phase a pour objectifs de :

- Collecter un maximum d'informations sensibles concernant les services accessibles et les équipements d'infrastructure associés à l'aide de diverses techniques (Les techniques doivent être communiquées) ;
- Identifier les vulnérabilités présentes sur les machines offrant ces services ;
- Tentatives d'exploitation de vulnérabilités et d'escalade de privilèges
- Dresser la liste des potentielles exploitations des vulnérabilités détectées et évaluer les risques d'intrusion dans les systèmes de LPEE ;
- Évaluer le niveau d'exposition des systèmes d'information face à une attaque externe sans information préalable (attaquant externe réel) ;
- Vérifier la présence d'éventuelles fuites d'information ou de mauvaises configurations accessibles depuis l'extérieur ;
- Évaluer la robustesse et la résilience de l'infrastructure de sécurité périmétrique (pare-feu, filtrage, cloisonnement, etc.) à travers des mises à l'épreuve simulant divers scénarios de menace ;
- Identifier les vecteurs d'attaque exploitables par un attaquant n'ayant aucun accès privilégié ;
- Evaluer les impacts potentiels et risques encourus ;

➤ **Démarche**

Cette phase d'audit sera menée selon les étapes suivantes :

- La description de la démarche et outils utilisés, et le périmètre retenu, ainsi que les risques couverts ;
- La définition et la qualification des différents tests effectués et des moyens utilisés ;
- Définition des outils et les techniques de détection des vulnérabilités et d'évaluation de leurs impacts sur le SI ;
- L'appréciation du niveau de sécurité du périmètre retenu par rapport aux normes et référentiels en la matière.
- Proposition d'actions correctives et préventives nécessaires.
- L'audit doit être effectué selon les deux modes des tests d'intrusion (boîte noire, boîte blanche).

➤ **Livrables**

- Rapport détaillé des tests externes en précisant :
 - La description des risques potentiels ;
 - Les conséquences potentielles ;
 - L'impact des vulnérabilités recensées sur la sécurité.

Etape 2 : Tests d'intrusion Internes

➤ **Objectif**

Le prestataire réalisera un audit complet en se déplaçant physiquement sur les sites concernés de LPEE. Maîtrisant l'architecture et l'organisation du SI, il disposera des informations nécessaires sur la configuration pour mener à bien les tests d'intrusion. L'objectif est de simuler une attaque provenant d'un utilisateur légitime ou d'un acteur malveillant ayant un accès privilégié.

Les principaux objectifs de cette étape sont les suivants :

- Analyser en profondeur l'architecture du système d'information, y compris les flux de données, les points de concentration, les interfaces critiques, et les mécanismes d'interconnexion entre les composants ;
- Identifier les vulnérabilités internes et les failles dans les mécanismes de sécurité internes ;
- Faire apparaître les failles et les risques conséquents d'intrusions (tentatives de fraude, accès et manipulation illicites de données, interception de données critiques, Ecoute réseau, Déni d'accès ...), ainsi que celles virales ;
- Mettre en évidence les vulnérabilités que pourrait exploiter un individu malveillant se situant à l'intérieur du SI, avec un certain niveau de connaissance préalable du réseau et avec des accès applicatifs ;
- Tenter d'exploiter les vulnérabilités réseau, système, applicatives et des risques détectés ;
- Évaluer la gestion des accès et des privilèges, et qu'aucune élévation abusive des droits n'est possible ;
- Tester les mécanismes de journalisation et de détection d'anomalies, afin de s'assurer que toute action suspecte est correctement tracée et signalée ;
- Évaluer la résilience face à un acteur interne malveillant, qu'il s'agisse d'un employé mécontent ou d'un utilisateur disposant d'un accès légitime mais abusif.

➤ **Démarche**

Cette phase d'audit sera menée selon les étapes suivantes :

- La description de la démarche et outils utilisés, et le périmètre retenu, ainsi que les risques couverts ;
- La définition et la qualification des différents tests effectués et des moyens utilisés ;
- Définition des outils et les techniques de détection des vulnérabilités et d'évaluation de leurs impacts sur le SI ;
- L'appréciation du niveau de sécurité du périmètre retenu par rapport aux normes et référentiels en la matière.

- Proposition d'actions correctives et préventives nécessaires.
- L'audit doit être effectué selon les deux modes des tests d'intrusion (boite noire, boîte blanche).

➤ **Livrables**

- Rapport détaillé de tests d'intrusion internes en précisant :
 - La description des risques potentiels ;
 - Les conséquences potentielles ;
 - L'impact des vulnérabilités recensées sur la sécurité.

PHASE 3 : Audit organisationnel

➤ **Objectif**

Cette phase d'audit organisationnel de la sécurité du SI a pour objectif de réaliser une analyse préliminaire de la situation actuelle (opérationnel et en cours de mise en place) en matière de management- de la sécurité de l'information sur le périmètre défini, d'identifier les points forts et les axes d'amélioration afin d'élaborer une démarche de mise en conformité de :

- La gouvernance de sécurité des systèmes d'information (SSI)
- La gestion des accès et habilitations
- La gestion des incidents de sécurité
- La gestion des risques cybersécurité
- La sensibilisation et formation des utilisateurs
- La cyber-résilience et continuité d'activité
- Les politiques, procédures, plans, et chartes sécurité SI.
- La conformité réglementaire et normative (Loi 05-20/09-08, DNSSI, ISO 27001/27002/27005, RGPD, etc.)

Cette étape permettra également d'évaluer tous les éléments (techniques, organisationnels, opérationnels, etc.) nécessaires au renforcement du niveau de sécurité des SI notamment :

- Évaluation des aspects organisationnelles liées à la gestion de la sécurité pour l'ensemble des activités ;
- Évaluation de l'efficacité de l'organisation des équipes de sécurité, notamment en ce qui concerne le périmètre des responsabilités et la répartition des rôles ;
- Évaluation de la capacité des équipes techniques à réagir efficacement aux enjeux de sécurité ;
- Évaluation des risques et formulation de recommandations adaptées pour la mise en œuvre de mesures organisationnelles en se basant sur la norme ISO 27005, et élaborer une cartographie des risques du SI ;
- Définition de la probabilité réelle, de l'impact résiduel et de la criticité des risques ;
- Définition des mesures et facteurs permettant l'atténuation et la réduction des risques identifiés ;
- Sécurité des supports de sauvegarde des données, des applications, et des archives ;
- Évaluation de la conformité des datacenters et des locaux informatiques aux normes internationales en matière de sécurité environnementale et physique.

➤ Démarche

Evaluer la conformité selon les exigences convenues

- Loi-05-20, loi-09-08, DNSSI, ISO 27001/27005, ISO22301, ... ;

Audit légal et réglementaire

- Cadrage et identification de l'exigence légale (Loi 05-20, Loi 09-08, ...);
- Revue documentaire et entretiens nécessaires ;
- Evaluation des écarts selon la réglementation retenue ;
- Evaluation des écarts par rapport aux norme internationaux (ISO 27001/27002/27005, NIST, ...);
- Rapport de conformité et restitution ;
- Evaluation des dispositifs de sécurité physique et environnementale ;

➤ Livrables

- Rapport détaillé de l'audit organisationnel, précisant notamment les éléments suivants :
 - Une synthèse des résultats
 - Les recommandation et plan d'action détaillé ;
 - Formulaire bien remplis exigés par la CNDP ;
- Rapport détaillant les écarts relevés par rapport aux exigences réglementaires (Loi-05-20, loi-09-08, DNSSI) ;
- Un framework d'évaluation de risque selon la méthodologie EBIOS RM ;

PHASE 4 : Audit de configuration & Architecture

➤ Objectifs

L'objectif de cette étape est de réaliser une évaluation technique de la configuration des composants du SI afin de s'assurer que les mesures de sécurité déployées respectent les bonnes pratiques en matière de sécurité.

Cette étape permettra aussi de réaliser une évaluation technique de l'architecture : vérifier le schéma d'architecture global, séparation des environnements (développement, test, production), redondance, segmentation, cloisonnement, interconnexions internes et externes, revue des flux critiques.

Audit de l'architecture :

Il s'agit de réaliser une analyse approfondie de l'infrastructure réseau, portant notamment sur le paramétrage et le positionnement des équipements et logiciels de filtrage, de détection, ainsi que des hôtes et dispositifs d'interconnexion. L'objectif est de vérifier la conformité aux bonnes pratiques et normes en matière de sécurité, notamment en ce qui concerne l'emplacement des actifs réseau et de sécurité, le cloisonnement, la gestion des flux, les réseaux sans fil, et autres éléments critiques.

Audit de configuration :

L'objectif de cet audit de configuration est d'évaluer la complétude des fichiers de configuration et de vérifier leur conformité aux meilleures pratiques dans le domaine. Cette analyse vise à identifier d'éventuelles faiblesses et à proposer des ajustements de paramétrage permettant de les corriger. Par ailleurs, le titulaire devra procéder à l'analyse et à la revue des configurations des composants de SI de LPEE.

Démarche

Le prestataire est tenu de vérifier, conformément à l'état de l'art ou aux exigences normatives et règles spécifiques de LPEE, la sécurité et la configuration des éléments suivants :

- Configuration des équipements réseaux, équipements de sécurité (pare-feu, switch, routeur, ...), architecture logique, plan d'adressage, détection automatique de vulnérabilités, liens télécoms etc ;
- Configuration des serveurs et des applications : dispositifs de sécurité, authentification, mise à jour et patch, systèmes d'exploitation, services réseau, ports d'accès aux services, messagerie, bases de données, accès à distance, gestion des profils et privilèges, système de consolidation des logs ;
- Evaluation des mécanismes de contrôle des accès et paramétrage des serveurs, postes clients, les hyperviseurs de virtualisation, durcissement système, ... ;
- Les évaluations de configuration doivent être conformes aux bonnes pratiques et aux références reconnues ;

➤ Livrable

- La liste détaillée des vulnérabilités, classifiées en fonction de leur gravité potentielle (conséquences, facilité d'exploitation...);
- Rapport d'audit d'architecture et de configuration, en détaillant les éléments suivants ;
 - Description des configurations analysées ;
 - Résultats de l'évaluation de la conformité ;
 - Analyse des risques associés aux faiblesses détectées ;
 - Matrice des écarts (Gap Analysis)
- Un design d'architecture de sécurité élaboré en tenant compte des failles de sécurité identifiées, du dimensionnement du réseau ainsi que des nouvelles menaces auxquelles il faudrait faire face ;

PHASE 5 : Feuille de route, plan d'action SSI et recommandations

➤ OBJECTIFS

Durant cette phase le prestataire devra produire une synthèse consolidée des constats de l'audit, incluant :

- Une synthèse des constats et un plan d'action ;
- La liste détaillée des vulnérabilités identifiées, accompagnée des méthodes utilisées pour les détecter ;
- Une qualification précise des failles détectées, associée à une évaluation des risques et impacts potentiels sur le système d'information ;
- Une synthèse des recommandations pour remédier à ces vulnérabilités, en lien avec les objectifs de sécurité définis ;

Sur la base de cette analyse, le prestataire devra élaborer un plan d'action structuré, comprenant :

- Des actions correctives ciblées pour chaque vulnérabilité, classées par ordre de priorité selon leur impact sur la gravité des scénarios de risques, leur coût, et les contraintes de mise en œuvre ;

- Des mesures urgentes, à la fois organisationnelles et techniques, à mettre en œuvre immédiatement pour corriger les défaillances critiques, y compris :
 - La mise à jour de l'architecture technique,
 - L'évolution des systèmes ;
 - Le renforcement du matériel ;
 - L'amélioration de la sécurité des locaux informatique, etc. ;

Le prestataire doit aussi définir les actions à mener, visant notamment :

- L'organisation de la sécurité du SI ;
- La mise en conformité par rapport aux lois et normes internationales de cybersécurité (ISO 27001/27005, DNSSI, loi 05-20, 09-08, etc.) ;
- L'intégration des outils et mécanismes de sécurité adéquats, accompagnée d'une estimation budgétaire ;

Le prestataire devra également proposer une feuille de route détaillée de la sécurité des Systèmes d'information du LPEE, couvrant une période de trois (3) ans et assortie d'un calendrier prévisionnel.

➤ Démarche

Validation des constats et résultats avec l'équipe De LPEE :

- Revue des constats et finalisation des recommandations ;
- Revue des actions correctives et préventives ;

Conception du plan d'action et feuille de route de sécurité SI :

- Qualification des constats d'audit et priorisation des recommandations ;
- Intégration des actions de remédiations visant à améliorer la sécurité en prenant en considération l'impact et le risque liés à chaque vulnérabilité ;
- Elaboration d'une feuille de route détaillée de la sécurité des systèmes d'information de LPEE sécurité à appliquer sur le court et moyen terme ;

➤ Livrables

- Plan d'action détaillé **priorisé et budgétisé**, couvrant des risques encourus ;
- Feuille de route de la sécurité des systèmes d'information de LPEE ;
- Politique de sécurité du Système d'Information ;
- Charte de sécurité du SI pour les simples utilisateurs ;

Le prestataire devra proposer une méthodologie détaillée de suivi opérationnel de la sécurité du système d'information, incluant les mécanismes de pilotage (tableaux de bord, gouvernance projet), les outils de surveillance, ainsi que les indicateurs de performance (KPI) jugés pertinents. Cette proposition devra permettre de définir les dispositifs de mesure continue de niveau de sécurité, de détection des écarts éventuels et de pilotage central pour la direction et des responsables sécurité.

PHASE 6 : Formation et transfert de compétences

Le titulaire doit assurer une formation et transfert de compétence sur le management de l'audit de de sécurité SI selon CISA ou la norme ISO 27001 lead auditor, pour un groupe minimum de cinq (4) personnes sur une durée de cinq (5) jours.

Le titulaire doit assurer également une formation pour la gestion des risques liés à la sécurité de l'information selon la norme ISO 27005 (3 jours).

Le prestataire doit mettre en place toutes les mesures permettant de mettre en bonnes conditions le personnel de LPEE participant aux sessions de formation

Article 38: Définition des prix

LOT 1 : AUDIT DE SECURITE DU SYSTEME D'INFORMATION DU LABORATOIRE PUBLIC
D'ESSAIS ET D'ETUDES - EN LOT UNIQUE

Prix n°1.1 : Le Cadrage et structuration du projet

Ce prix rémunère le Cadrage et structuration du projet selon les spécifications de l'article 30 du présent marché, y compris tous frais de main d'œuvre, transport et toutes sujétions nécessaires pour la prestation de services.

Prix rémunéré au forfait.....(F)

Prix n°1.2 : Audit de sécurité technique

Ce prix rémunère l'audit de sécurité technique selon les spécifications de l'article 30 du présent marché, y compris tous frais de main d'œuvre, transport et toutes sujétions nécessaires pour la prestation de services.

Prix rémunéré au forfait.....(F)

Prix n°1.3 : Audit organisationnel

Ce prix rémunère l'audit organisationnel selon les spécifications de l'article 30 du présent marché, y compris tous frais de main d'œuvre, transport et toutes sujétions nécessaires pour la prestation de services.

Prix rémunéré au forfait.....(F)

Prix n°1.4 : Audit de configuration et Architecture

Ce prix rémunère l'Audit de configuration et Architecture selon les spécifications de l'article 30 du présent marché, y compris tous frais de main d'œuvre, transport et toutes sujétions nécessaires pour la prestation de services.

Prix rémunéré au forfait.....(F)

Prix n°1.5 : Feuille de route et plan d'action SSI

Ce prix rémunère la Feuille de route et plan d'action SSI selon les spécifications de l'article 30 du présent marché, y compris tous frais de main d'œuvre, transport et toutes sujétions nécessaires pour la prestation de services.

Prix rémunéré au forfait.....(F)

Prix n°1.6 : Formation et transfert de compétences

Ce prix rémunère la Formation et transfert de compétences selon les spécifications de l'article 30 du présent marché, y compris tous frais de main d'œuvre, transport et toutes sujétions nécessaires pour la prestation de services.

Prix rémunéré au forfait.....(F)

BORDEREAU DES PRIX – DETAIL ESTIMATIF**LOT 1 : AUDIT DE SECURITE DU SYSTEME D'INFORMATION DU LABORATOIRE PUBLIC
D'ESSAIS ET D'ETUDES**

N° de prix	Désignation	Unité	Quantité	Prix unitaire en DH/HT	Prix total en DH/HT
1	Cadrage et structuration du projet	F	1		
2	Audit de sécurité technique	F	1		
3	Audit organisationnel	F	1		
4	Audit de configuration et Architecture	F	1		
5	Feuille de route et plan d'action SSI	F	1		
6	Formation et transfert de compétences	F	1		
MONTANT TOTAL HT					
TVA (20%)					
MONTANT TOTAL TTC					

Fait à, le

(Signature et cachet du prestataire de services)

DERNIERE PAGE

APPEL D'OFFRES OUVERT SUR OFFRES DE PRIX N°62/2025

OBJET : AUDIT DE SECURITE DU SYSTEME D'INFORMATION DU LABORATOIRE PUBLIC D'ESSAIS ET D'ETUDES - EN LOT UNIQUE

POUR UN MONTANT DE (en chiffres et en lettres) :

Le Prestataire de services	Le Maître d'ouvrage
<p>Nom et qualité du signataire</p> <p>Lu et approuvé (<i>mention manuscrite</i>)</p> <p>Cachet et signature</p>	<p align="center">DOSI</p> <div data-bbox="922 660 1364 817"> </div> <p align="center">DLAAP</p> <p align="center">PRESENTE PAR : F. OUTERGA</p> <div data-bbox="1093 907 1300 974"> </div> <p align="center">VERIFIE PAR : H. SARJANE</p> <div data-bbox="965 1108 1268 1377"> </div> <p align="center">LA DIRECTION GENERALE DU LPEE</p> <div data-bbox="949 1467 1252 1814"> </div>