

- Microsoft 365 et outils collaboratifs ;
- Infrastructure virtualisée et services d'hébergement ;
- Solutions de cybersécurité.

L'augmentation des cybermenaces, les exigences réglementaires nationales ainsi que les enjeux liés à la protection des données imposent la mise en place d'un SMSI conforme aux meilleures pratiques internationales.

Dans cette perspective, l'AMMPS souhaite développer une expertise interne capable de piloter la conception, le déploiement, l'amélioration continue et la certification d'un SMSI.

3. Cadre réglementaire

La prestation devra être réalisée conformément aux référentiels et normes suivants :

Référentiels internationaux

- ISO/IEC 27001:2022 – Information Security Management Systems – Requirements ;
- ISO/IEC 27002:2022 – Information Security Controls ;
- ISO/IEC 27005 – Information Security Risk Management ;
- ISO 31000 – Risk Management ;
- ISO 19011 – Guidelines for Auditing Management Systems ;

Référentiels nationaux

- Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) ;
- Guides et recommandations publiés par la DGSSI ;
- Réglementation marocaine applicable aux systèmes d'information et à la cybersécurité.

L'organisme de formation devra démontrer que son contenu pédagogique est aligné sur ces référentiels et couvre les principaux domaines du cursus Lead Implementer.

4. Objectifs de la formation

a. Objectif général

Permettre aux participants d'acquérir les connaissances théoriques, méthodologiques et pratiques nécessaires pour mettre en œuvre un SMSI conforme à la norme ISO/IEC 27001 : 2022 et piloter une démarche de certification.

b. Objectifs spécifiques

À l'issue de la formation, les participants devront être capables de :

- Interpréter les exigences de la norme ISO/IEC 27001:2022 ;
- Comprendre les exigences des normes ISO/IEC 27002, ISO/IEC 27005 et ISO 31000 ;

- Définir le contexte d'un SMSI ;
- Identifier les parties intéressées ;
- Déterminer le périmètre d'un SMSI ;
- Conduire une analyse des écarts (Gap Analysis) ;
- Réaliser une analyse et un traitement des risques ;
- Élaborer une Déclaration d'Applicabilité (SoA) ;
- Sélectionner et justifier les mesures de sécurité applicables ;
- Élaborer les politiques et procédures du SMSI ;
- Préparer un audit interne ;
- Préparer une revue de direction ;
- Accompagner une certification ISO/IEC 27001.

5. Résultats attendus

À l'issue de la prestation, l'AMMPS devra disposer de collaborateurs capables de :

- Piloter un projet de mise en œuvre d'un SMSI ;
- Assurer la conformité du SMSI aux exigences de l'ISO/IEC 27001 ;
- Conduire des ateliers d'analyse de risques ;
- Élaborer les principaux documents du SMSI ;
- Accompagner les audits de certification ;
- Assurer l'amélioration continue du système de management.

Les participants devront également être préparés à l'examen officiel Lead Implementer et disposer des connaissances nécessaires pour obtenir la certification.

6. Public cible

La formation est destinée aux cadres impliqués dans la gouvernance, la sécurité et la transformation numérique de l'AMMPS, notamment :

- Responsables Infrastructure ;
- Responsables Réseaux ;
- Responsables Cybersécurité ;
- Chefs de projets SI ;
- Administrateurs Systèmes et Réseaux ;
- Responsables Qualité ;
- Responsables Gestion des Risques ;
- Auditeurs internes ;
- Responsables RH ;
- Toute personne amenée à participer à la mise en œuvre d'un SMSI.

7. Durée de la prestation

La durée minimale de la formation est fixée à cinq (05) jours, représentant environ 40 heures de formation. Le calendrier de la formation sera programmé en commun accord entre le soumissionnaire et l'équipe AMMPS.

Chaque journée comprendra des exposés théoriques, des exercices pratiques, des études de cas et des séances de questions-réponses.

Le dernier jour sera consacré en partie à la préparation de l'examen officiel.

8. Modalités d'organisation

La formation sera dispensée en présentiel dans les locaux de l'AMMPS ou dans un centre de formation proposé par le prestataire et validé par l'AMMPS. Le prestataire est tenu de prendre en charge totalement les frais de formation y compris toute logistique y afférente (pause déjeuner...).

Le nombre prévisionnel de participants est de 10 à 15 personnes.

La langue de formation sera le français. Les supports pourront être fournis en français ou en anglais.

Le prestataire devra mettre à disposition :

- Les supports pédagogiques ;
- Les exercices ;
- Les études de cas ;
- Les examens blancs ;
- Les documents de référence ;
- Les attestations de participation.

II. PRESCRIPTIONS TECHNIQUES ET PÉDAGOGIQUES

9. Consistance de la prestation

La prestation porte sur la conception, l'organisation et l'animation d'une formation certifiante ISO/IEC 27001:2022 Lead Implementer, destinée aux cadres de l'AMMPS impliqués dans la gouvernance, la sécurité et la transformation numérique.

Le prestataire retenu devra assurer l'ensemble des prestations nécessaires à la bonne réalisation de cette mission, notamment :

- La préparation pédagogique de la formation ;
- La mise à disposition d'un formateur certifié PECB ou équivalent ;
- La fourniture des supports pédagogiques ;
- L'animation des sessions de formation ;
- L'encadrement des travaux pratiques ;
- La préparation des participants à l'examen officiel ;
- L'organisation des évaluations intermédiaires ;

- L'inscription des participants à l'examen de certification ;
- La remise des attestations de participation.

La formation devra combiner des apports théoriques, des exercices pratiques, des études de cas et des ateliers collaboratifs afin de favoriser l'acquisition de compétences directement exploitables dans le contexte de l'AMMPS.

10. Programme pédagogique détaillé

Le programme proposé devra être conforme aux exigences de la norme ISO/IEC 27001:2022 et couvrir l'ensemble des domaines de compétences nécessaires à la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI).

Le contenu ci-après constitue le minimum attendu.

Jour 1 – Introduction aux systèmes de management de la sécurité de l'information

Cette première journée devra permettre aux participants de comprendre les principes fondamentaux de la sécurité de l'information et les exigences générales de la norme ISO/IEC 27001.

Le programme abordera notamment :

- Les enjeux de la cybersécurité ;
- Les principes de gouvernance de la sécurité de l'information ;
- La famille des normes ISO/IEC 27000 ;
- Les exigences de l'ISO/IEC 27001:2022 ;
- La structure harmonisée (HLS) des normes ISO ;
- Les concepts de confidentialité, intégrité et disponibilité ;
- Les notions de menace, vulnérabilité, risque et impact ;
- Les parties intéressées ;
- Les exigences réglementaires ;
- La définition d'un SMSI.

Travaux pratiques

Les participants devront réaliser :

- L'identification des actifs informationnels d'une organisation ;
- L'analyse des parties intéressées ;
- La définition du périmètre d'un SMSI.

Jour 2 – Planification et conception du SMSI

Cette journée sera consacrée à la planification du projet de mise en œuvre.

Le prestataire devra présenter notamment :

- Le rôle de la Direction Générale ;
- La gouvernance du SMSI ;
- Les rôles et responsabilités ;
- L'analyse de l'existant (Gap Analysis) ;
- La politique de sécurité ;

- Les objectifs du SMSI ;
- Les indicateurs de performance ;
- Les exigences documentaires ;
- La planification des ressources.

Gestion des risques

Le prestataire devra développer :

- ISO 31000 ;
- ISO/IEC 27005 ;
- Méthodes d'analyse des risques ;
- Critères d'acceptation des risques ;
- Traitements des risques ;
- Plans de traitement.

Atelier

Les participants devront réaliser une analyse de risques sur un cas inspiré des activités de l'AMMPS.

Jour 3 – Mise en œuvre du SMSI

Cette journée devra porter sur la phase opérationnelle de mise en œuvre.

Le prestataire présentera notamment :

- La gestion documentaire ;
- Les procédures obligatoires ;
- Les politiques de sécurité ;
- La déclaration d'applicabilité (statement of applicability) ;
- La sélection des mesures de sécurité ;
- La justification des exclusions ;
- Les contrôles de l'annexe a ;
- La sensibilisation des utilisateurs ;
- La communication interne ;
- La gestion des incidents ;
- La gestion des changements.

Atelier pratique

Chaque participant devra élaborer :

- Un extrait de politique de sécurité ;
- Un registre des risques ;
- Une matrice de traitement des risques ;
- Une déclaration d'applicabilité simplifiée.

Jour 4 – Exploitation, surveillance et amélioration

Le prestataire présentera :

- Le suivi des performances du SMSI ;
- Les indicateurs de sécurité ;
- Les audits internes ;
- Les non-conformités ;
- Les actions correctives ;
- La revue de direction ;
- L'amélioration continue.

Travaux pratiques

Les participants devront :

- Construire un programme d'audit interne ;
- Préparer une revue de direction ;
- Analyser plusieurs non-conformités ;
- Élaborer un plan d'actions.

Jour 5 – Préparation à la certification

Cette journée sera consacrée à la préparation de l'examen officiel.

Le prestataire devra présenter :

- Le processus de certification ISO/IEC 27001 ;
- Les différentes étapes de l'audit ;
- Les attentes des auditeurs ;
- Les erreurs fréquemment constatées ;
- Les bonnes pratiques de mise en œuvre.

Examen blanc

Le prestataire organisera :

- Un examen blanc dans les conditions réelles ;
- Une correction collective ;
- Une séance de questions-réponses.

11. Travaux pratiques

La formation devra privilégier une approche opérationnelle.

Les travaux pratiques devront représenter au minimum 40 % du volume horaire.

Ils devront porter notamment sur :

- L'identification des actifs ;
- L'analyse des parties intéressées ;
- La cartographie des processus ;
- La définition du périmètre du SMSI ;

- L'analyse des écarts ;
- La gestion des risques ;
- La rédaction de politiques de sécurité ;
- L'élaboration de la déclaration d'applicabilité ;
- La sélection des mesures de sécurité ;
- La préparation d'un audit interne ;
- La conduite d'une revue de direction.

Les exercices devront être contextualisés autant que possible aux activités d'un établissement public tel que l'AMMPS.

12. Études de cas

Le prestataire proposera plusieurs études de cas couvrant notamment :

- La mise en œuvre d'un SMSI dans une administration publique ;
- La sécurisation d'un système d'information de santé ;
- La gestion d'un incident de cybersécurité ;
- La gestion des risques liés à un projet cloud ;
- La préparation d'un audit de certification.

Les études de cas devront permettre aux participants d'appliquer les exigences de l'ISO/IEC 27001 dans des situations réalistes.

13. Méthodologie pédagogique

Le prestataire devra adopter une démarche pédagogique active et participative comprenant :

- Des exposés illustrés ;
- Des ateliers collaboratifs ;
- Des études de cas ;
- Des travaux en groupe ;
- Des quiz d'évaluation ;
- Des échanges d'expérience.

La pédagogie devra favoriser le transfert des connaissances vers les projets de l'AMMPS et préparer efficacement les participants à la certification.

14. Supports pédagogiques

Le prestataire fournira, pour chaque participant :

- Un manuel de formation complet ;
- Les supports de présentation ;
- Les exercices pratiques ;
- Les corrigés ;
- Les modèles de documents du SMSI ;

- Des modèles de politiques de sécurité ;
- Un modèle de registre des risques ;
- Un modèle de déclaration d'applicabilité.

Tous les supports seront remis en version électronique (PDF) et, si prévu dans l'offre, en version papier.

III. EXIGENCES RELATIVES AU PRESTATAIRE, LIVRABLES, MODALITÉS D'EXÉCUTION ET ÉVALUATION DES OFFRES

15. Qualification des formateurs

Le formateur principal proposé devra satisfaire aux exigences minimales suivantes :

Formation

- Certification ISO/IEC 27001 Lead Implementer en cours de validité.
- Certification ISO/IEC 27001 Lead Auditor (souhaitable).
- Certification ISO/IEC 27005 Risk Manager (souhaitable).
- Certification ISO 31000 Risk Manager (souhaitable).

Expérience

Le formateur devra justifier :

- D'au moins huit (8) années d'expérience professionnelle dans le domaine de la gouvernance de la sécurité de l'information.
- Une expérience dans le secteur public ou dans les secteurs de la santé, de l'industrie pharmaceutique ou des laboratoires constituera un atout.

16. Moyens pédagogiques

Le prestataire devra mettre à disposition :

- Un environnement pédagogique adapté ;
- Des supports numériques de qualité ;
- Un espace de partage documentaire ;
- Des études de cas ;
- Des examens blancs ;
- Des questionnaires d'évaluation.

Les supports devront être remis aux participants avant le démarrage de la formation.

17. Livrables attendus

Le titulaire remettra au minimum les livrables suivants :

N°	Livrable	Format
1	Support complet de formation	PDF
3	Exercices pratiques	PDF / Word
4	Études de cas	PDF
5	Corrigés des exercices	PDF
6	Examen blanc	PDF
7	Corrigé de l'examen blanc	PDF
8	Fiches d'évaluation des participants	PDF
9	Attestations de participation	Papier et PDF

18. Rapport de fin de formation

À l'issue de la mission, le prestataire transmettra un rapport comprenant notamment :

- Le déroulement de la formation ;
- Le taux de participation ;
- Les résultats des évaluations ;
- Les difficultés rencontrées ;
- Les recommandations pour la suite du projet SMSI ;
- Les résultats de l'examen blanc ;
- Le taux de réussite prévisionnel.

19. Modalités d'exécution

Le prestataire devra désigner un chef de projet unique qui sera l'interlocuteur de l'AMMPS.

Avant le démarrage de la mission, une réunion de lancement sera organisée afin de :

- Valider le calendrier ;
- Confirmer la liste des participants ;
- Arrêter les modalités logistiques ;
- Définir les responsabilités respectives.

Pendant toute la durée de la mission, le prestataire assurera un suivi régulier avec le chef de projet désigné par l'AMMPS.

20. Assurance qualité

Le prestataire devra mettre en œuvre un dispositif qualité garantissant :

- La conformité du contenu pédagogique ;
- Le respect du planning ;
- La qualité des supports ;
- La disponibilité des formateurs ;
- La satisfaction des participants.

L'AMMPS pourra procéder à tout moment à une évaluation qualitative de la prestation.

21. Critères de réception

La prestation sera considérée comme réceptionnée après :

- La réalisation complète de la formation ;
- La remise de l'ensemble des supports ;
- La transmission du rapport de fin de formation ;
- La remise des attestations de participation ;
- La validation des livrables par l'AMMPS.

En cas de non-conformité, le prestataire devra procéder aux corrections demandées sans coût supplémentaire.

22. Critères d'évaluation des offres techniques

L'offre technique :

Les soumissionnaires doivent présenter une offre technique faisant ressortir leur capacité à réaliser la prestation de formation. A cet effet, ils doivent fournir, les documents suivants :

1.Document 1 : Note méthodologique pour la conduite du programme de formation proposé

- Le soumissionnaire présentera en détail son approche méthodologique pour l'exécution de la prestation de formation et sa capacité logistique et organisationnelle suffisante pour assurer la prestation dans les délais impartis

2.Document 2 : Existence légale de l'organisme de formation

- Document(s) justifiant l'existence légale d'au moins cinq (5) années de l'organisme de formation et sone expérience dans l'organisation de formations certifiantes ISO/IEC 27001 Lead Implementer.

3.Document 3 : Attestations de référence

- Trois attestations de référence auprès d'administrations publiques, d'établissements publics ou de grandes entreprises dont l'objet est similaire à la prestation de formation demandée.

4.Document 4 : Le CV, le(s) copies de(s) diplôme(s) et le(s) certification(s) du formateur :

- Être titulaire d'un diplôme Bac +5 en informatique, ou réseaux, ou télécoms, ou sécurité des SI ;
- Ayant une expérience d'au moins 8) années d'expérience professionnelle dans le domaine de la gouvernance de la sécurité de l'information (une expérience dans le secteur public ou dans les secteurs de la santé, de l'industrie pharmaceutique ou des laboratoires constituera un atout) ;
- Certifications : Formateur certifié PECB, ISO/IEC 27001 Lead Implementer en cours de validité, ISO/IEC 27001 Lead Auditor (souhaitable), ISO/IEC 27005 Risk Manager (souhaitable), ISO 31000 Risk Manager (souhaitable).

Les offres techniques seront évaluées selon les critères suivants :

Critère	Points
Qualité et pertinence du programme proposé	20
Expérience de l'organisme	10
Qualification du formateur principal	40
Études de cas et travaux pratiques	15
Modalités de préparation à la certification	15

Seuil technique

Toute offre ayant obtenu une note technique inférieure à 70/100 sera écartée.

23. Confidentialité

Le titulaire est tenu à une obligation stricte de confidentialité concernant toutes les informations auxquelles il aura accès dans le cadre de la mission.

À ce titre, il s'engage à :

- Ne divulguer aucune information relative à l'AMMPS ;
- Utiliser les informations exclusivement dans le cadre de la prestation ;
- Restituer ou détruire tout document à la demande de l'AMMPS.

Cette obligation demeure applicable après l'achèvement de la mission.

24. Propriété intellectuelle

Tous les supports spécifiques développés pour l'AMMPS dans le cadre de cette mission deviendront la propriété de l'AMMPS.

Le prestataire conserve toutefois les droits sur ses supports pédagogiques standards et sur les contenus protégés appartenant à des organismes tiers, sous réserve d'accorder à l'AMMPS un droit d'utilisation interne conformément aux licences applicables.

25. Obligations du titulaire

Le titulaire s'engage notamment à :

- Respecter le calendrier validé ;
- Mobiliser les experts annoncés dans son offre ;
- Assurer la continuité pédagogique ;
- Informer immédiatement l'AMMPS de toute difficulté susceptible d'affecter la prestation ;
- Remplacer tout intervenant indisponible par un profil de qualification équivalente, après accord préalable de l'AMMPS.

26. Pénalités

En cas de retard imputable au titulaire ou de non-respect des engagements contractuels, l'AMMPS pourra appliquer les pénalités prévues par la réglementation des marchés publics et les stipulations du contrat.

IV. CLAUSES CONTRACTUELLES, SUIVI DE LA PRESTATION ET ANNEXES

27. Gouvernance de la prestation

Afin d'assurer le bon déroulement de la mission, une gouvernance sera mise en place entre l'AMMPS et le titulaire.

Comité de pilotage

Le comité de pilotage est chargé de :

- Valider le calendrier d'exécution ;
- Suivre l'état d'avancement de la prestation ;
- Examiner les difficultés rencontrées ;
- Statuer sur les éventuelles demandes d'ajustement ;
- Valider les livrables.

Le comité est composé notamment :

- Du Chef de division des Systèmes d'Information ou son représentant ;
- Du chef de projet désigné par l'AMMPS ;
- Du formateur principal.

Le comité pourra se réunir à tout moment sur demande de l'une des parties.

28. Planning prévisionnel

Le titulaire proposera un planning détaillé comprenant au minimum :

Phase	Durée
Formation	5 jours
Examen blanc	1 jour

Le calendrier définitif sera validé conjointement avec l'AMMPS.

29. Obligations de l'AMMPS

L'AMMPS s'engage à :

- Désigner un interlocuteur unique ;
- Communiquer au titulaire la liste définitive des participants ;
- Mettre à disposition les locaux si la formation est organisée dans ses locaux ;
- Faciliter l'accès aux informations nécessaires à la bonne exécution de la mission ;
- Assurer la disponibilité des participants pendant toute la durée de la formation.

30. Obligations du titulaire

Le titulaire est tenu notamment de :

- Respecter le planning validé ;
- Assurer la qualité pédagogique de la formation ;
- Mobiliser les experts annoncés dans son offre ;
- Respecter les règles de sécurité applicables au sein de l'AMMPS ;
- Informer immédiatement l'AMMPS de toute difficulté susceptible d'affecter le déroulement de la mission.

Toute substitution d'un formateur devra être préalablement approuvée par l'AMMPS. Le remplaçant devra présenter un niveau de qualification et d'expérience au moins équivalent.

31. Protection des informations

Le titulaire reconnaît que les informations auxquelles il pourra avoir accès sont susceptibles de présenter un caractère sensible.

À ce titre, il s'engage à :

- Respecter la confidentialité des informations ;
- Ne copier aucun document sans autorisation écrite ;
- Ne conserver aucune donnée après la fin de la mission ;
- Restituer l'ensemble des documents transmis.

L'AMMPS pourra exiger la signature d'un engagement individuel de confidentialité par chaque intervenant.

32. Protection des données personnelles

Lorsque la mission implique le traitement de données à caractère personnel, le titulaire s'engage à :

- Respecter la réglementation marocaine applicable ;
- Appliquer les mesures techniques et organisationnelles nécessaires à la protection des données ;
- Limiter le traitement aux seules informations nécessaires à l'exécution de la prestation ;
- Notifier sans délai toute violation de données constatée.

33. Assurance

Le titulaire devra être couvert par une assurance responsabilité civile professionnelle couvrant les conséquences financières des dommages pouvant résulter de l'exécution de la prestation.

Une attestation en cours de validité pourra être demandée avant la notification du marché.

34. Force majeure

Aucune des parties ne pourra être tenue responsable d'un retard ou d'une inexécution résultant d'un cas de force majeure tel que défini par la législation en vigueur.

La partie concernée devra informer l'autre partie dans les meilleurs délais.

35. Résiliation

L'AMMPS pourra résilier le marché dans les cas prévus par la réglementation applicable, notamment en cas de :

- Retard important non justifié ;
- Inexécution des obligations contractuelles ;
- Abandon de la prestation ;
- Remplacement non autorisé du personnel clé ;
- Manquements répétés à la qualité des prestations.

La résiliation pourra être prononcée après mise en demeure restée sans effet.

36. Règlement des différends

Les parties s'efforceront de régler à l'amiable tout différend relatif à l'exécution du marché.

À défaut d'accord amiable, les juridictions administratives compétentes seront seules compétentes.

37. Réception des prestations

La réception définitive sera prononcée après :

- La réalisation complète de la formation ;
- La remise des livrables contractuels ;
- La validation du rapport final ;
- La levée des éventuelles réserves.

En cas de réserves, le titulaire disposera d'un délai fixé par l'AMMPS pour procéder aux corrections demandées.

38. Indicateurs de performance (KPI)

Le titulaire devra atteindre les objectifs suivants :

Indicateur	Objectif
Taux de présence	≥ 95 %
Satisfaction des participants	≥ 90 %
Respect du planning	100 %
Livrables remis dans les délais	100 %
Réclamations majeures	0

Ces indicateurs pourront être utilisés par l'AMMPS pour apprécier la qualité de la prestation.

V. MODE ET DATE DE PAIEMENT

Le contrat sera établi dans le cadre du programme d'appui du Fonds mondial - Maroc - subvention 2024-2026. Les modalités et calendrier de paiement seront définis dans le contrat.

La rémunération s'entend :

- Brute avant déduction de la retenue à la source de 11% par la banque pour les personnes physiques et morales-consultants étrangers et 30% pour les personnes physiques-consultants résidents au Maroc.
- Nette pour les Autoentrepreneurs et les personnes morales-consultants résidents au Maroc. Le Ministère se charge des démarches auprès de la DGI pour l'obtention de l'attestation d'exonération sur la base de la facture proforma à préparer par le consultant.

VI. PIÈCES À FOURNIR

Tout(e) candidat(e) intéressé(e) devra envoyer le dossier, au plus tard **le 10 Aout 2026 à minuit**, à l'adresse suivante : Direction de l'Epidémiologie et de Lutte contre les Maladies, UGFM, 71, Avenue Ibn Sina, Agdal, Rabat ; ou aux adresses électroniques : mounir.eljanati@ammmps.gov.ma, aymen.hafid@ammmps.gov.ma et f.gomri@programmefondsmondial.ma, en mettant dans l'objet de l'email : **TDR Formation CERTIFIANTE ISO/IEC 27001 : 2022 Lead Implementer au profit de l'agence marocaine des médicaments et des produits de santé (AMMPS)**

Le dossier doit comprendre :

- Programme détaillé de la formation ;
- Planning proposé ;
- CV détaillés des formateurs ;
- Copies des certifications.
- Une note méthodologique pour la conduite de la formation ;
- Une proposition financière.

