Projet financé par l'Union européenne

Projet de coopération technique sur la mobilité professionnelle circulaire

THAMM II

Opérateur de mise en œuvre

Sélection d'un Prestataire pour l'Audit de Sécurité du Système d'Information Intégré dédié à la Formation Professionnelle Privée (SIGAF)

Cadre : Coopération technique entre la Tunisie et l'Union européenne

Contractant : Représentation en Tunisie de l'Office français de l'immigration et de l'intégration (OFII, opérateur de mise en œuvre de THAMM OFII)

Zone géographique d'intervention : Tunisie

1. Contexte :

Le projet THAMM OFII est un projet de coopération technique dans le domaine de la mobilité professionnelle circulaire, conçu de manière conjointe par l'Agence nationale pour l'emploi et le travail indépendant (ANETI, Tunisie) et l'Office français de l'immigration et de l'intégration (OFII).

L'OFII lance la présente consultation auprès **des prestataires certifiées par l'Agence Nationale de la Cybersécurité – ANCS** en vue de la réalisation d'une mission d'audit de sécurité du système d'information intégré destiné à dématérialiser et automatiser les processus métiers relatifs aux activités de la formation professionnelle privée (SIGAF). Ce système d'information intégré est une solution logicielle en cours de développement et mise en place progressive en quatre (04) lots .

2. Lots de la consultation :

La consultation est structurée en **quatre (04) lots non dissociables**, chacun représentant un ensemble de fonctionnalités, soit déjà développées et prêtes pour audit (lot 1), soit à développer et à mettre en production progressivement au cours de l'année 2025 (lots 2, 3 et 4).

Les offres techniques et financières des soumissionnaires doivent impérativement couvrir les quatre (04) lots de développement. De ce fait, aucune offre ne peut être soumise pour un seul lot.

Les lots 2, 3 et 4 seront livrés en moyenne tous les deux mois et demi calendaires à partir de la deuxième quinzaine de mars 2025, avec une finalisation des travaux de développement et une recette fonctionnelle globale prévue pour la fin octobre 2025.

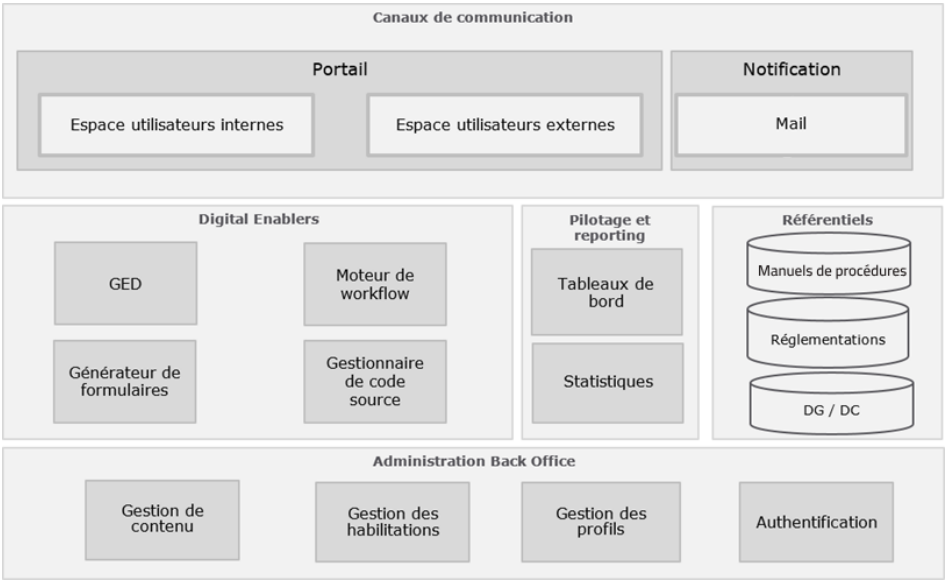
La mission objet de la présente consultation devra impérativement être clôturée avant le 31/12/2025.

L'intervention du prestataire sélectionné sera après la finalisation des travaux de développement de chaque lot afin de préparer sa validation pour l'hébergement auprès des fournisseurs internet et cloud gouvernementaux.

La cartographie fonctionnelle se compose des blocs suivants :

- **Chaîne de valeur :** ensemble des étapes permettant de formaliser les processus de la formation professionnelle (solution dotée d'un moteur de workflow conforme à la norme BPMN 2.0 permettant de gérer et couvrir l'ensemble des processus métiers) ;
- **Canaux de communication :** ensemble des moyens mis à disposition des utilisateurs de la plateforme, pour interagir entre eux, échanger des informations et des documents, etc. ;
- **Administration Back Office :** ensemble de fonctionnalités à assurer permettant le paramétrage, la gestion et la supervision de la solution ;
- **Pilotage :** ensemble de rapports et de statistiques à générer par la plateforme ;
- **Gestion des référentiels :** ensemble des référentiels de données gérés au niveau de la plateforme.

La cartographie fonctionnelle en question est modélisée ci-après :



Pour chaque lot, deux livrables seront prévus :

- Le premier, sous la forme d'un rapport détaillé d'audit, couvrant les différents aspects spécifiés dans la présente consultation, devra inclure les résultats de l'estimation des risques, les mesures techniques à mettre en œuvre ainsi que les grandes lignes du plan d'action.
- Le deuxième livrable sera un rapport de conformité aux exigences techniques et recommandations formulées dans le premier rapport après l'intervention corrective de la société de développement. Dans le cas où le premier rapport ne révèle aucune exigence ou recommandation à traiter, le deuxième rapport ne sera pas nécessaire.

3. Conduite et déroulement de la mission d'audit :

L'audit devra suivre les phases décrites dans les paragraphes suivants.

3.1 Déclenchement de l'audit :

Le déclenchement de l'audit sera marqué par une réunion préparatoire entre l'équipe de projet, l'équipe de développement et le prestataire. Au cours de cette étape, il y a lieu de traiter des aspects suivants :

- Etablir les circuits de communication ;
- Rappeler le contexte de l'audit et son importance pour l'identification et l'atténuation des risques relatifs à la sécurité de l'information, ainsi que l'étendue et les limites de l'audit (les processus couverts par l'audit). Il sera important de présenter la méthodologie utilisée par le prestataire et de distinguer les activités d'audit qui auront lieu sur site de celles qui seront conduites à distance, et ce en commun accord avec le maitre d'ouvrage ;
- Affiner les plannings d'exécution (planning des actions, plannings des réunions de coordination et de synthèse, etc.) ;
- Définir et prendre les dispositions logistiques nécessaire à la mission du prestataire (au ministère et sur le site de développement, etc.).

Cette réunion débouchera sur la synthèse des plannings précis et détaillés de mise en œuvre de la mission qui seront consignés dans un PV.

En cas de difficultés, le prestataire devra faire recours à l'équipe projet (ministère et OFII) par courriel, afin de leur permettre d'intervenir efficacement et dans les délais.

3.2 Conduite des activités d'audit

Audit technique :

L'audit technique vise à évaluer le niveau de sécurité des lots de développement du système d'information décrit ci-dessus.

L'audit devra suivre les étapes suivantes :

- ✓ Audit Black Box.
- ✓ Audit Grey Box.
- ✓ Audit White Box.

La méthodologie proposée par le soumissionnaire pour la conduite de l'audit technique devra, entre autres, inclure :

- Une méthode d'évaluation de la sécurité de l'architecture adoptée dans l'environnement de développement ;
- Une méthode d'évaluation de la sécurité des lots de développement du système d'information ;
- Une méthode pour la réalisation des tests d'intrusion externe (réalisés depuis Internet) ;
- Une méthode pour la réalisation des tests d'intrusion interne (réalisés depuis le réseau intranet du ministère) ;
- Une méthode pour la réalisation des tests d'intrusion applicatifs ;
- Une analyse et évaluation des risques.

Le soumissionnaire devra proposer, dans son offre, une méthodologie d'analyse et d'évaluation des risques qui sera utilisée pour estimer le risque lié à chaque faille détectée durant l'audit. Cette méthodologie devra prendre en considération des facteurs tels que la criticité de l'actif touché par la faille, l'impact d'exploitation de la faille et la probabilité de son occurrence.

Cette méthodologie permettra également de classer les failles découvertes durant l'audit selon le niveau de risque.

Outils d'audit :

Le soumissionnaire devra décrire dans son offre les outils techniques qu'il compte utiliser lors de la réalisation de l'audit qui doivent comprendre :

- ✓ Des outils de sondage et de scan de vulnérabilités ;
- ✓ Des outils de scan automatique des vulnérabilités du réseau ;
- ✓ Des outils spécialisés dans l'audit des SGBD ;
- ✓ Des outils de test de la solidité des objets d'authentification (fichiers de mots clés, etc.).

L'utilisation d'outils commerciaux devra être accompagnée de la présentation d'une copie de la licence originale et nominative permettant leur usage correct pour de telles missions (inexistence de restrictions quant à leur usage pour les audits : plages d'adresses ouvertes, etc.). **La présentation de la copie des licences en question sera requise uniquement du prestataire retenu avant signature du contrat**.

Il est à noter qu'en plus des points mentionnés ci-dessus, le prestataire devra se conformer aux critères techniques d'audit ainsi qu'aux modalités de suivi de la mise en œuvre des recommandations définies dans le référentiel d'audit de sécurité des systèmes d'information disponible sur le site officiel de l'Agence Nationale de la Cybersécurité à l'URL suivante : https://www.ancs.tn/fr/audit/demarche.

Les exigences liées aux modalités et outils spécifiés dans ce référentiel, **relatives à l'audit des applicatifs et solutions logicielles** pour la réalisation de la mission objet de cette consultation, feront partie intégrante du périmètre et ne pourront être ignorées.

3.3 Livrables attendus :

Les livrables de la présente mission d'audit sont :

- PV de lancement du projet incluant particulièrement les plannings d'exécution ;

Pour chacun des lots décrits ci-dessus,

- Livrable 1 : Rapport détaillé d'audit intégrant en particulier les résultats de l'estimation des risques, les mesures techniques à mettre en œuvre ainsi que les grandes lignes du plan d'action (conformément aux aspects mentionnés dans le paragraphe 3.2).
- Livrable 2 : Rapport de conformité aux exigences techniques et recommandations formulées dans le premier rapport après l'intervention de la société de développement. Dans le cas où le livrable 1 ne révèle aucune exigence ou recommandation à traiter, ce deuxième livrable ne sera pas nécessaire.

Il est à noter que les livrables seront soumis à la validation de l'organisme en charge de l'hébergement de l'environnement de production du système d'information. En cas de réserve, le prestataire est tenu de procéder à ses frais, à la correction des manquements et/ou non conformités signalés.

4. Modalités de paiement :

Les modalités de paiement seront définies selon le calendrier suivant :

- 25% à la validation du PV de la réunion du lancement et des livrables relatifs au lot 1.

- 25% à la validation des livrables relatifs au lot 2.

- 25% à la validation des livrables relatifs au lot 3.

- 25% à la validation des livrables relatifs au lot 4.

Ces modalités de paiement peuvent être affinées, si besoin est, en commun accord avec le prestataire lors de la contractualisation.

5. Profil souhaité de(s) l'expert(s) ou de(s) collaborateur(s) en charge de la mission :

Critère	Exigence minimale de l'expert principal désigné comme point focal	En cas de proposition d'autres membres
Cas où le prestataire est une personne morale	Société figurant dans la liste officielle des personnes morales certifiées sur publiée sur le site web de l'agence, accessible à l'adresse suivante : https://www.ancs.tn/fr/audit/experts-auditeurs Il est à noter que, dans ce cas **où le prestataire est une personne morale**, l'expert principal proposé comme point focal doit figurer dans la même liste officielle des experts appartenant à cette société.	

Critère	Exigence minimale de l'expert principal désigné comme point focal	En cas de proposition d'autres membres
Cas où le prestataire est une personne physique	Expert certifié par l'Agence Nationale de la Cybersécurité, figurant dans la liste officielle des experts certifiés publiée sur le site web de l'agence, accessible à l'adresse suivante : https://www.ancs.tn/fr/audit/experts-auditeurs	
Nombre d'année d'expérience	Une expérience de 05 ans.	Une expérience de 03 ans.
Certification valides	Être certifié Lead Implémenter ISO/IEC 27001 **ou** Lead Auditeur ISO/IEC 27001 Et Avoir au minimum 1 certification parmi les suivantes : ✓ Certified Information System Security professionnal(CISSP) ✓ Certified Information System Manager (CISM)	Être certifié Lead Implémenter ISO/IEC 27001 **ou** Lead Auditeur ISO/IEC 27001 Une certification parmi les suivantes **sera un plus :** ✓ Certified Information System Manager (CISM) ✓ EC-Council CEH ✓ Certified Information ✓ System Security Professionnal (CISSP)
Nombre de participation aux projets similaires	Doit avoir participé à au moins 6 missions de tests d'intrusion.	Chaque membre de l'équipe Intervenante doit avoir participé à au moins 3 missions de tests d'intrusion.
Expérience spécifique :	Une référence de collaboration avec un projet de coopération technique internationale. Une référence de collaboration avec le ministère de l'Emploi et de la Formation professionnelle sera considérée comme un plus.	Une référence de collaboration avec un projet de coopération technique ou avec le ministère de l'Emploi et de la Formation professionnelle sera considérée comme un plus.

6. Modalités de soumission des candidatures :

Dossier de candidatures :

Les prestataires intéressés sont invités à soumettre leur dossier de candidature avec les éléments suivants :

- ✓ Le/les curriculum(s) vitae détaillé(s) mettant en évidence l'expérience pertinente de l'expert ou de(s) collaborateur(s) du prestataire dans le domaine requis avec les références requises.
- ✓ L'offre technique
- ✓ La copie du registre national de l'entreprise (RNE).
- ✓ Une offre financière.

Si un ensemble de prestataires souhaitent former une équipe pour participer à cette consultation, ils doivent désigner l'un d'eux comme responsable principal, qui représentera leur candidature comme un seul prestataire. Ce responsable sera le point de contact unique vis-à-vis de l'OFII et assumera l'organisation administrative, fiscale et juridique de l'équipe. La facturation sera effectuée en son nom, et il supportera directement la charge de tous les impôts, droits et taxes auxquels il est soumis, de quelque nature qu'ils soient.

Envoi des dossiers

Les dossiers de candidature doivent être envoyés avec la référence **« Audit de sécurité du système d'information (SIGAF) »** dans l'objet du courriel, aux adresses suivantes : thammofii@gmail.com , saber.neffati@ofii.fr et helene.hammouda@ofii.fr.

La date limite de réception des candidatures est le 24/12/2024 avant minuit.