REPUBLIQUE TUNISIENNE
Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université de Kairouan

PAQ – DGSU

Projet : Appui & renforcement de la gestion stratégique de l'Université de Kairouan afin de promouvoir l'autonomie, la redevabilité & la performance : « INITIATIVE VERS L'EXCELLENCE »

TERMES DE RÉFÉRENCE

Appel à Manifestation d'Intérêt N° 08/2023 PAQ-DGSU

Recrutement d'un cabinet de service et d'ingénierie informatique pour la mission :

"Audit et politique de sécurité du SI de l'université de Kairouan"

Références PAQ-DGSU

A1.3.2-2 : Réaliser un audit du Système d'information de l'Université de Kairouan et un établissement Pilote.
A1.3.2-3 : Elaborer et mettre en place une politique de sécurité de SI.

SOMMAIRE

I. CONTEXTE DU PROJET

Le ministère de l'Enseignement Supérieur et de la Recherche Scientifique (MESRS) met en œuvre un Projet de Modernisation de l'Enseignement Supérieur en soutien à l'Employabilité des jeunes diplômés (PromESsE) financé en partie par la Banque Internationale pour la Reconstruction et le Développement (Accord de prêt n° 8590-TN). Dans ce cadre, le MESRS a lancé un nouveau Fonds d'Innovation : le PAQ pour le Développement de la Gestion Stratégique des Universités (PAQ-DGSU) avec l'objectif de faciliter et d'accélérer la migration des universités publiques vers davantage d'autonomie institutionnelle, de redevabilité et de performance. Le Fonds PAQ-DGSU vise en particulier à appuyer chaque université bénéficiaire dans son propre projet de modernisation et s'articule autour des notions suivantes :

- L'auto-évaluation institutionnelle, pour mesurer ses forces et faiblesses sur une base réaliste et dégager des pistes de développement ;
- Le Plan d'Orientation Stratégique, pour afficher ses priorités de développement ;
- Le Contrat avec le MESRS, qui concrétise l'engagement de l'État sur des objectifs de progrès partagés avec l'université bénéficiaire ;
- Le financement basé sur la performance, qui incite l'université bénéficiaire à améliorer son efficacité dans la mise en œuvre du contrat et à la maintenir.

Dans ce contexte, l'Université de Kairouan a reçu une allocation PAQ pour le financement de son projet PAQ-DGSU « ***Appui & renforcement de la gestion stratégique de l'Université de Kairouan afin de promouvoir l'autonomie, la redevabilité & la performance*** ».

Dans ce cadre, l'Université de Kairouan va confier à un cabinet de service et d'ingénierie informatique pour la mission :

« Audit et politique de sécurité du SI de l'université de Kairouan »

II. OBJECTIFS DE LA MISSION

L'université de Kairouan se propose de lancer Manifestation auprès des sociétés de service et d'ingénierie informatique en vue de la réalisation d'une mission d'audit de la sécurité de son système d'information conformément au décret N°2004-1250, du 25 Mai 2004, et aux dispositions du présent cahier des charges, piloté par au moins un chef de projet certifié par l'Agence Nationale de la Sécurité Informatique, conformément au décret 1249-2004 du 25

mai 2004. **Le chef du service Informatique et son équipe de l'université de Kairouan doivent être impliqués dans la totalité des phases du projet sous forme de transfert de compétences**.

III. DEFINITIONS ET INTERPRETATIONS

Maître d'Ouvrage	Désigne L'université de Kairouan et englobe les structures ou personnes dûment mandatées pour la supervision de cette mission.
Soumissionnaire	Désigne toute personne morale ayant retiré les documents de la manifestation d'intêret N° 08/2023 PAQ-DGSU et avoir soumis une offre en réponse à ces documents à titre individuel ou solidaire avec d'autres personnes morales.
Titulaire	Désigne l'entreprise dont la soumission a été retenue par le Maître d'Ouvrage et englobe les représentants, successeurs et ayants droits légaux dudit prestataire.
Mission	Signifie toute action d'audit, de test, de vérification y compris la rédaction des rapports, les déplacements, la collecte de données, l'analyse des tests, et toute autre action assurée par le titulaire pour le compte du Maître d'Ouvrage dans le cadre de la bonne exécution de la manifestation d'intêret.
Un audit de sécurité	Consiste à valider les moyens de protection mis en œuvre sur les plans organisationnels, procéduraux et techniques, au regard de la politique de sécurité en faisant appel à un tiers de confiance expert en audit sécurité informatique. L'audit de sécurité conduit, au-delà du constat, à analyser les risques opérationnels pour le domaine étudié, et par la suite à proposer des recommandations et un plan d'actions quantifiées et hiérarchisées pour corriger les vulnérabilités et réduire l'exposition aux risques.
Système d'information	Désigne l'ensemble des entités et moyens (structures, personnel, procédures, outils logiciels, équipements de traitement, équipements réseaux, équipements de sécurité, bâtiments, ...) en relation avec les fonctions de traitement de l'information.
ANSI	Désigne l'Agence Nationale de la Sécurité Informatique.

IV. CONDITIONS DE PARTICIPATION

Cette Manifestation s'adresse aux entreprises certifiées par l'Agence Nationale de la sécurité Informatique conformément au décret 2004-1249 du 25 mai 2004. Et conformément à l'arrêté du ministre des Technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité informatique. (La liste actualisée est disponible sur le site web www.ansi.tn).

V. PRESENTATION ET RECEPTION DES OFFRES

Le dossier de la soumission doit nécessairement être constitué de l'**offre technique** et de **l'offre financière.**

Toute offre parvenue après le dernier délai de réception des offres sera rejetée. L'enveloppe doit contenir : Les pièces administratives de l'offre et l'offre technique.

4.1 Les pièces administratives

L'offre du soumissionnaire doit renfermer l'ensemble des pièces administratives suivantes :

• Une copie conforme du certificat du soumissionnaire en cours de validité,

• La déclaration trimestrielle des salariés et des salaires de la CNSS du dernier trimestre avant la date limite de remise des offres, des trois (3) auditeurs certifiés par l'ANSI et employés à temps plein par le soumissionnaire,

• Les Déclarations sur l'honneur de confidentialité du soumissionnaire et des auditeurs qui seront impliqués, éventuellement, dans les réunions d'éclaircissement et de visite sur terrain, préliminaires à la soumission de l'offre (**annexe 6**).

4.2 offre technique

L'enveloppe contenant le dossier technique doit comporter les pièces suivantes :

• Le cahier des charges et ses annexes avec paraphe et cachet humide au bas de chaque page. La signature de la dernière page doit être précédée de la date et de la mention manuscrite « Lu et approuvé »,

• Un aperçu succinct sur l'activité générale du soumissionnaire, son organisation et son expérience dans le domaine,

• Présentation des références du soumissionnaire (**selon le modèle fourni dans l'Annexe 1**),

• Présentation de l'équipe intervenante (**selon le modèle fourni dans l'Annexe 2**),

• Méthodologie(s) proposée(s) pour la conduite de l'audit incluant la spécification des outils logiciels d'accompagnement (traitement des enquêtes et calcul de risque) conforme au référentiel établi par l'ANSI

• Descriptif des opérations de sensibilisation, accompagné des références des intervenants et d'une description de la matière de sensibilisation (documents/maquettes, …) qui sera utilisée,

• Le calendrier global d'exécution, spécifiant clairement toutes les phases d'exécution, accompagné des modèles de l'**Annexe 3** y afférents, remplis avec précision,

• Les CVs et références de l'équipe d'audit proposée, conformément au modèle fourni en **Annexe 7**, accompagnés de toutes les pièces justificatives nécessaires,

• Présentation des Outils techniques utilisés, conformément au modèle fourni en **Annexe 4**.

VI. METHODE DE SELECTION

La sélection du cabinet de consultants comme étant le soumissionnaire (organismes d'accompagnement et de consulting, bureau d'études, de formation et d'expertise etc.) est effectuée conformément aux procédures définies dans les directives « Sélection et Emploi de Consultants par les Emprunteurs de la Banque Mondiale » éditées en janvier 2011 et mises à jour en juillet 2014. Pour cette mission, un bureau de consultants sera choisi selon la méthode de sélection fondée sur les Qualifications des Consultants (QC).

Les cabinets de consultants sont invités à se faire connaître et à fournir des informations sur leurs expériences et leurs compétences en rapport avec la nature de la mission. Une liste restreinte sera établie. Le cabinet ayant les qualifications et références les plus adéquates, sera choisi pour la mission. **Le cabinet de consultants retenu sera invité à négocier son offre**.

Une commission de sélection (CS) du projet établira un classement des soumissionnaires selon le barème de notation présenté dans le tableau suivant :

	Critères d'évaluation	**Détails des critères d'évaluation**	**Note**	**Total**
01	Expérience du cabinet	Expérience et mission justifiée (02 points pour chaque mission) (max 10pts). Minimum 7 ans d'expérience dans le domaine de la sécurité (5pts). 1 points par année d'expérience (au-delà des 7 ans) (max 5pts).	20/100	**20 points /100**

02	Expérience du chef du projet	Expérience Générale, Diplôme et Expérience similaire. Certifié ANSI, ISO27001 Lead Auditor, ISO27005 - Minimum 15 ans d'expérience en sécurité de l'information (8pts) - Minimum 5 références d'audit réglementaire (5pts) - Employé à plein temps (5pts) 4 points par mission d'audit réglementaire pendant les 3 dernières années (12pts)	30/100	**30 points /100**
03	Expérience de l'équipe 3 consultants min. Employés à plein temps au niveau de l'entreprise	Un consultant en sécurité de l'information certifié ANSI + ISO27005 ou ISO27001 avec 10 ans d'expérience. (4pts) 2 points par mission d'audit réglementaire pendant les 3 dernières années (max 6pts)	10/100	**30 points /100**
		Un consultant en sécurité de l'information certifié ANSI + CEH ou ISO27001 avec 5 ans d'expériences. (4pts) 2 points par mission d'audit réglementaire pendant les 3 dernières années (max 6pts)	10/100	
		Un consultant spécialiste Continuité d'activité certifié ANSI + ISO22301 ou CISA avec 10 ans d'expériences. (4pts) 2 points par mission d'audit réglementaire pendant les 3 dernières années (max 6pts)	10/100	
04	Planning et outils	Planning prévisionnel de la mission – conformité du planning avec les objectifs de la mission	10/100	**20 points /100**
		Méthodologie de travail. Pertinence de la méthodologie avec le contexte de la mission	10/100	
Total				**100/100**

Le score technique minimum requis pour être classé dans la liste restreinte est de **70/100** points. Toute candidature ayant un score nul dans l'un des trois premiers critères ci-dessus mentionnés sera éliminée de la sélection, et ce indépendamment de son score final. Le dossier doit être appuyé par toutes les pièces justificatives, en effet toute information qui nécessite un éclaircissement ne sera pas prise en considération que si la pièce de justification sera présentée et ceci après l'accord de la commission d'évaluation, dans un délai de 10 jours pour compléter le dossier.

La commission va procéder à l'ouverture de l'offre du candidat le mieux classé. Le bureau du consultant classé premier sera invité à remettre une proposition technique détaillée et une offre financière. Une invitation à une séance de négociation sera adressée à ce candidat avant minimum 7 jours ouvrables, les négociations porteront essentiellement sur :

Les conditions techniques de mise en œuvre de la mission, notamment le calendrier détaillé de déroulement de la mission. L'approche méthodologique, le contenu des livrables et l'offre financière.

VII. CONFLITS D'INTERETS

Les cabinets en conflits d'intérêt, c'est-à-dire qui auraient un intérêt quelconque direct ou indirect au projet ou qui sont en relation personnelle ou professionnelle avec la Banque Mondiale ou le MESRS, doivent déclarer leurs conflits d'intérêt au moment de la transmission de la lettre de candidature pour la mission. En particulier, tout fonctionnaire exerçant une fonction administrative doit présenter les autorisations nécessaires pour assurer la mission.

VIII. CONFIDENTIALITE

Le cabinet de consultants retenu pour la présente mission est tenu de respecter une stricte confidentialité vis-à-vis des tiers, pour toute information relative à la mission ou collectée à son occasion. Tout manquement à cette clause entraîne l'interruption immédiate de la mission. Cette confidentialité reste de règle et sans limitation après la fin de la mission.

IX. COMPOSANTES DU PROJET

Ce projet d'assistance comporte plusieurs phases. Un soumissionnaire doit soumettre pour toutes les phases qui sont les suivantes :

Phase 1. Audit réglementaire de la sécurité du SI :

Cette mission aura pour objectif de procéder à un audit sécurité du système d'information de l'entreprise dans un souci d'une meilleure protection et performance de l'utilisation de l'information. Cette phase se déroulera en deux étapes. Une première étape relative à l'organisation générale de l'université de Kairouan en ce qui concerne les aspects liés à l'organisation de la sécurité de l'information et une deuxième étape relative à l'analyse et le diagnostic de la sécurité du réseau et des systèmes.

Ces étapes doivent être réalisées comme suit :

- ***<u>Etape 1 : Audit organisationnel et physique</u>***

Il s'agit, pour ce volet d'évaluer les aspects organisationnels de gestion de la sécurité de la structure objet de l'audit, d'estimer les risques et de proposer les recommandations adéquates pour la mise en place des mesures organisationnelles et d'une politique sécuritaire adéquate. On s'intéressera aux aspects de gestion et d'organisation de la sécurité sur les plans organisationnels, humains et physiques.

Au cours de cette étape, le prestataire devra emprunter une approche méthodologique, basée sur des batteries de questionnaires préétablis et adaptés à la réalité des entités auditées, permettant d'aboutir à une évaluation pragmatique des failles et des risques encourus, ainsi qu'à, bien entendu, l'identification et classification des ressources relatives à leur critique.

Cet audit devra prendre comme référentiel tous les chapitres (domaines) de la dernière version de la norme ISO/IEC 27002 (version 2013). Ci-dessous les différents points de contrôle (conformément à l'ISO27002) à vérifier :

- Chapitre n° 5 : Politiques de sécurité de l'information
- Chapitre n° 6 : Organisation de la sécurité de l'information
- Chapitre n° 7 : La sécurité des ressources humaines
- Chapitre n° 8 : Gestion des actifs
- Chapitre n° 9 : Contrôle d'accès
- Chapitre n° 10 : Cryptographie
- Chapitre n° 11 : Sécurité physique et environnementale
- Chapitre n° 12 : Sécurité liée à l'exploitation
- Chapitre n° 13 : Sécurité des communications
- Chapitre n° 14 : Acquisition, développement et maintenance des systèmes d'information
- Chapitre n° 15 : Relations avec les fournisseurs
- Chapitre n° 16 : Gestion des incidents liés à la sécurité de l'information
- Chapitre n° 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Chapitre n° 18 : Conformité

- ***Etape 2 : Diagnostic technique***

NB : Les données volumétriques relatives aux infrastructures à auditer sont détaillées en ***Annexe 5***

Ce volet concerne l'audit technique de l'architecture de sécurité. Il s'agit de procéder à une analyse très fine de l'infrastructure sécuritaire des systèmes d'information et particulièrement du réseau. Cette analyse devra faire apparaître les failles et les risques conséquents d'intrusions actives (tentatives de fraude, accès et manipulation illicites de données, interception de données critiques…), ainsi que celles virales ou automatisées , et ce suite à divers tests de vulnérabilité conduits dans le cadre de cette mission, qui doivent englober des opérations de simulation d'intrusion et tous autres tests permettant d'apprécier la robustesse de la sécurité des systèmes d'information et leur capacité à préserver les aspects de confidentialité, d'intégrité , de disponibilité et d'autorisation.

Au cours de cette étape, le prestataire devra, en réalisant des audits techniques de vulnérabilités, des tests et simulations d'attaques réelles :

- Dégager les écarts entre l'architecture réelle et celle décrite lors des entretiens ou dans la documentation, ainsi qu'entre les procédures techniques de sécurité supposées être appliquées (interviews) et celles réellement mise en œuvre.

- Evaluer, la vulnérabilité et solidité des composantes matérielles et logicielles du système d'information (réseau, systèmes, mécanismes d'administration et de gestion, plates-formes matérielles...), contre toutes les formes de fraude et d'attaque connues par les spécialistes du domaine au moment où l'audit est conduit, et touchant les aspects de confidentialité, intégrité et disponibilité des informations (et le cas échéant, celles des mécanismes d'autorisation (authentification, certification ..) Et de non-répudiation.

- Evaluer l'herméticité des frontières du réseau, contre les tentatives de son exploitation par des attaquants externes (sites d'amplification d'attaque, relais de spam, exploitation du PABX pour le détournement (« vol ») des lignes de communication …).

Elle devra aussi inclure une évaluation des mécanismes et outils de sécurité présentement implémentés et diagnostiquer et tester toutes leurs failles architecturales et techniques,

ainsi que les lacunes en matière d'administration et d'usage de leurs composantes logicielles et matérielles.

Les tests réalisés ne devront pas mettre en cause la continuité du service du système audité. Les tests critiques, pouvant provoquer des effets de bord, devront être notifiés au chef de projet (coté maître d'ouvrage) et devront, si nécessaire, être réalisés sous sa supervision, conformément à un planning préalablement établi et validé, et qui pourra concerner des horaires de pause et éventuellement de chôme.

- ***Etape 3 : Analyse de risque***

Dans cette phase et après avoir identifié les failles de sécurité organisationnelles, physiques et techniques, il s'agit de suivre une approche méthodologique pour évaluer les risques encourus et leurs impacts sur la sécurité de la structure auditée.

La phase d'analyse et d'évaluation du risque se déroulera en deux étapes.

La première étape permettrait la conduite d'une analyse afin :

1- Identifier les ressources critiques : les informations, les actifs matériels, les actifs logiciels, les personnels, …
2- Identifier les menaces auxquels sont confrontés ces actifs (intentionnelle ou non intentionnelle),
3- Identifier les vulnérabilités (au niveau organisationnel, au niveau physique et au niveau technique) qui pourraient être exploitées par les menaces,
4- Identifier les impacts que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs,
5- Evaluer la probabilité réaliste d'une défaillance de sécurité au vu des mesures actuellement mises en œuvre,

Par la suite, le cabinet d'audit est amené à :

1- Etablir une classification des risques par niveaux, et déterminer le niveau du risque acceptable,
2- Evaluer les risques, en fonction des facteurs identifiés dans la phase d'analyse, et les classifier par niveaux,
3- Identifier les mesures préventives et les mesures correctives de sécurité à implémenter pour éliminer ou réduire les risques identifiés.

Phase 2. Préparation d'une feuille de route sécurité

Le prestataire est invité, à la fin de la phase d'audit sur terrain de réaliser une synthèse, permettant l'établissement de la liste des failles (classées par ordre de gravité et d'impact), ainsi qu'une évaluation de leurs risques et une synthèse des recommandations conséquentes.

Les recommandations devront inclure au minimum :

- Les actions détaillées (organisationnelles et techniques) urgentes à mettre en œuvre dans l'immédiat, pour parer aux défaillances les plus graves.
- Les actions organisationnelles, physiques et techniques à mettre en œuvre sur le court terme (jusqu'à la date du prochain audit), englobant entre autres :
    - Les premières actions et mesures à entreprendre en vue d'assurer la sécurisation de l'ensemble du système d'information audité, aussi bien sur le plan physique que sur le plan organisationnel (structures et postes à créer, opérations de sensibilisation et de formation, procédures d'exploitation sécurisées à instaurer,) et technique (outils et mécanismes de sécurité à mettre en œuvre, incluant une référence aux opportunités et options offertes par les outils disponibles dans le monde du logiciel libre), ainsi qu'éventuellement des aménagements architecturaux de la solution de sécurité existante.
    - Une estimation des formations requises et des ressources humaines et financières supplémentaires nécessaires ;
    - La proposition de l'esquisse d'un premier schéma directeur cadre (sur trois années) ;
    - Préparation des spécifications techniques du matériel et solutions (informatique et réseau) à acquérir.

Phase 3. Mission de suivi post-audit (Optionnel)

Le prestataire devrait s'engager à proposer un forfait de 15 H/J dont l'objectif est d'implémenter des mesures de sécurités proposées dans le plan d'action. Ces mesures techniques peuvent concerner :

- Le développement de politiques / instruction tel que
    - Gestion des habilitations
    - Gestion des accès

- Gestion du filtrage
- …

Un minimum de 6 documents à développer (à convenir lors de la mission)

- Maitrise d'ouvrage :
  - Vérification et suivi de l'application des mesures de sécurité par les prestataires de l'entreprise

X. RAPPORTS ET RESULTATS ATTENDUES

Le consultant devrait fournir avec précision les outils qu'ils utiliseraient pour la phase de diagnostic du réseau de l'université de Kairouan. Il est ainsi tenu de donner une description détaillée de l'outil et des fonctionnalités qu'il peut offrir.

Les rapports et les résultats attendus sont :

I. Rapports et résultats attendues du projet

Les spécifications et les exigences liées à la réalisation de chaque activité sont détaillées ci-dessous :

Phase 1. Audit sécurité du SI :

- Rapport d'audit détaillé
- Rapport de synthèse
- Une politique de sécurité

Phase 2. Préparation d'une feuille de route sécurité

- Plan d'action sur 3 ans
- Budget et planning de mise en place de la solution

Phase 3. Mission de suivi post-audit

- Rapports d'interventions.

XI. DUREE D'EXECUTION DE LA MISSION

Phase 1. Audit sécurité du Système d'Information :

- Cette tâche d'assistance devra précéder toutes les autres tâches prévues dans le cadre de cette mission d'assistance
- La durée d'exécution de cette mission a été évaluée à 4 semaines

Phase 2. Préparation d'une feuille de route sécurité

- La durée d'exécution de cette mission a été évaluée à 4 semaines

Phase 3. Mission de suivi post-audit

- Cette tâche d'assistance est réalisée après la clôture des phases 1, 2 et 3 de la première année
- Cette tâche d'assistance est réalisée à partir de la deuxième année (pendant 3 ans)
- La durée d'exécution de cette mission a été évaluée à 5 semaines.

XII. PIECES CONSTITUTIVES DE LA MANIFESTATION D'INTÉRÊT

- Une lettre de candidature au nom du Président de l'Université de Kairouan ;
- Un Curriculum Vitae, selon le modèle joint en annexe des présents termes de référence, incluant toute information indiquant que le candidat atteste de l'expérience et des compétences nécessaires et qu'il est qualifié pour exécuter les prestations demandées ;
- Une liste des références du consultant dans des missions similaires ;
- Une copie des pièces justificatives (i) des diplômes, (ii) des expériences du candidat, et (iii) des qualifications du candidat en rapport avec la nature de la mission.
- Planning prévisionnel de la mission
- Présentation des Outils techniques utilisés
- Qualité des Moyens humains mis à la disposition

Les dossiers de candidature **peuvent** être présentés numériquement en pièces jointes via la plateforme TUNEPS **Ou bien** parvenir physiquement par voie postale ou par porteur à l'adresse ci-dessous avec la mention :

« Ne Pas Ouvrir, Appel à Manifestation N° 08/2023 PAQ-DGSU »

Recrutement d'un cabinet de service et d'ingénierie informatique pour la mission :

«Audit et politique de sécurité du SI de l'université de Kairouan»

Adresse : Université de Kairouan, Campus Universitaire, Route périphérique Dar El Amen Kairouan 3100. La date limite pour la réception des dossiers est fixée au **22/06/2023 à 10H00** (Le cachet du Bureau d'Ordre de l'Université de Kairouan faisant foi).

XIII. ANNEXES

ANNEXE 1

MODELE-Type de Présentation des offres

Ces modèles sont fournis pour servir comme modèles-types pour faciliter et normaliser la formulation des réponses. Chaque soumissionnaire est libre de les enrichir (et éventuellement d'en adapter la forme), afin de fournir toutes les informations requises pour le dépouillement.

Références du Soumissionnaire		
Ordre	Sous-critère	Réponse : Année / organisme : description [1]
1	Spécialisation de l'entreprise dans l'activité d'audit sécurité	
2	Spécialisation de l'entreprise dans L'activité de la sécurité Informatique (Intégration, Conseil, formation, ….)	
3	Nombre des missions d'audit sécurité, conformes au décret N° 2004-1250, de plus de 30 Jours, effectuées durant les trois dernières années.	

[1] Seules les missions justifiées par des P.V. de réception ou attestations du client seront considérées dans l'évaluation.

Annexe 2 : Planning prévisionnel de la mission

Composant		Equipe intervenante	Durée en Homme/jour pour Chaque intervenant		Logistique utilisée (Outils,…)	Livrable
Phase : Audit sécurité	Objet de la sous phase		Sur Site	Total		
Audit Organisationnel et physique	1: ……..	Nom:……				
	2: ……	Nom:……				
	n: ……	Nom:……				
Audit Technique	1: ……..	Nom:……				
	2: ……	Nom:……				
	n: ……	Nom:……				
Analyse des risques	1: ……..	Nom:……				
	2: ……	Nom:……				
	n: ……	Nom:……				
Politique de sécurité	1: ……..	Nom:……				
	2: ……	Nom:……				
	n: ……	Nom:……				
Durée Totale de la mission (en Homme/jour)						

Signature et cachet du soumissionnaire	
Noms et signatures de(s) auditeur(s) certifié(s)	

Annexe 3- Qualité des Moyens humains mis à la disposition de la mission

2.1-Présentation du Chef du Projet :

Nom et Prénom	Diplôme	Date d'obtention	Certificats obtenues ou formation (Année/ Titre/Organisme)	Les missions d'audit en tant que chef de projet (Année/nombre de jours/Organisme) [1]	Les missions d'audit en tant que membre (Année/nombre de jours /Organisme) [1]

2.2-Présentation des membres de l'équipe intervenante :

Nom et Prénom	Diplôme	Date d'obtention	Certificats Obtenues ou formation (Année/ Titre/Organisme)	Les missions d'audit ou missions de sécurité (Année/nombre de jours/Organisme) [1]	Les activités principales ou spécialités dans la mission

[1] Seules les missions justifiées par des P.V. de réception ou attestations du client seront considérées dans l'évaluation

Annexe 4 : Présentation des Outils techniques utilisés

Outils de : ……

Outils	Référence	Liste des fonctionnalités offertes ou à mettre en œuvre dans la mission	Utilité pour la mission	Lieu d'utilisation (Planning, phase)	Référence de la documentation dans le dossier de l'offre (éventuellement sous forme électronique : CD, ..)

ANNEXE 5: Description du système d'information de l'organisme

Type de composant (matériel/logiciel)	Description
Système de câblage	Système de câblage universel supportant l'informatique (Fibre et utp6)
Equipements actifs réseau informatique	5 Switchs Niveau 2 et 2 Switchs Niveau 3 et 2 Routeurs (CCK + CNI)
Serveurs	1 Blade + 2 serveurs Physiques et 10 serveurs virtuels
Systèmes d'exploitation serveur	Windows / linux / OSx
Progiciels	CRM / ERP / Intranet / Qualité / Application de Pointage / Supervision
Applications	Application de gestion des RH/ Application de Gestion du Recrutement / Applications de gestion développées en interne …
SGBD	HyperFileSQL
Equipement/Logiciel de sécurité logique	Active Directory Antivirus, Logiciel de sauvegarde et NAS, Firewall,
Sécurité Physique	Contrôle d'accès par badge pour la porte principale/ deux salles techniques/ Détecteurs de fumée/ 12 Caméras de surveillance
FTP	Serveur sftp
Ordinateurs/OS	70 PCs Client légers/ PCs portable/ OS Windows
Imprimantes	80 Imprimantes Laser / 3 Jet d'encre / 5 Photocopie / Fax
Equipement amovibles	Disque dur externe et CD/DVD pour l'équipe technique. dongles de licences
Equipements Wifi	8 points d'accès gérés par un contrôleur wifi

J'ATTESTE, EN TOUTE BONNE CONSCIENCE, QUE LES RENSEIGNEMENTS SUSMENTIONNES REFLETENT EXACTEMENT MA SITUATION, MES QUALIFICATIONS ET MON EXPERIENCE.
JE M'ENGAGE A ASSUMER LES CONSEQUENCES DE TOUTE DECLARATION VOLONTAIREMENT ERRONEE.

... . DATE: *JOUR / MOIS / ANNEE*
[Signature du consultant]

PAQ-PromESSE

ANNEXE 6: DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE

Je soussigné Mr/Mme ……, Responsable de la société ……..……..… déclare désigner Mr/Mme ……..……. Expert auditeur, certifié par l'Agence Nationale de la sécurité informatique et faisant partie de notre société, pour nous représenter dans la réunion d'éclaircissement sur le contenu du cahier de charges, et dans la phase préparatoire à la soumission de notre offre pour la manifestation d'intérêts ……

Le Soumissionnaire

(Cachet et signature)

ANNEXE 7: MODELE DE CURRICULUM VITAE

Annexe. CV pour la candidature pour la mission de …….

1. **Nom et prénom :**
2. **Date de naissance :** **Nationalité :**
3. **Niveau d'études :**

Institution (Dates : début – fin)	Diplôme(s) obtenu(s)
	▪
	▪
	▪
	▪

4. **Compétences clés :**
5. **Affiliation à des associations/groupements professionnels :**
6. **Autres formations**
7. **Pays où l'expert a travaillé :**
8. **Langues :** (bon, moyen, médiocre)

Langue	Lu	Parlé	Écrit

9. **Expérience professionnelle :**

Depuis - Jusqu'à	Employeur	Poste

10. **Compétences spécifiques de l'expert exigées dans le cadre de leur mission**

❶	Expérience
❷	Mission de formation similaire sur thèmes demandés

❸	Mission similaire dans le milieu universitaire et de la recherche scientifique

Détails de compétence spécifique à la mission	Expérience de l'expert qui illustre le mieux sa compétence pour la mission	
1	• Nom du projet : • Année : • Lieu : • Client : • Poste : • Activités	
2	• Nom du projet : • Année : • Lieu : • Client : • Poste : • Activités	
3	• Nom du projet : • Année : • Lieu : • Client : • Poste : • Activités	
4	• Nom du projet : • Année : • Lieu : • Client : • Poste : • Activités	

11. Information complémentaire

J'ATTESTE, EN TOUTE BONNE CONSCIENCE, QUE LES RENSEIGNEMENTS SUSMENTIONNES REFLETENT EXACTEMENT MA SITUATION, MES QUALIFICATIONS ET MON EXPERIENCE.
JE M'ENGAGE A ASSUMER LES CONSEQUENCES DE TOUTE DECLARATION VOLONTAIREMENT ERRONEE.

... . DATE: *JOUR / MOIS / ANNEE*
[Signature du consultant]

PAQ-PromESSE