CONSULTATION N° 98/2023

TERMES DE REFERENCES

« Audit de la sécurité du SMSI de Centre de Recherche en Numérique de Sfax»

Dernier délai d'acceptation des dossiers : 30 novembre 2023

1. Contexte de l'action

Le présent projet s'insère dans le cadre de la mise en place d'un dispositif de gouvernance des travaux de recherche au sein du CRNS. Ce dispositif a permis au CRNS de se certifier conformément à la norme ISO9001 (Qualité). Dans la continuité de cette stratégie, la CRNS a identifié un besoin de maitrise de la protection et de la sécurisation des données traités dans les travaux de recherche. En effet, ce besoin a été fortement évoqué et exprimé par les partenaires stratégiques du Centre de Recherche.

2. Objectifs de la mission

Dans le cadre du projet de mise en place d'un SMSI au niveau de la CRNS, le Centre de Recherche se propose de lancer une consultation dont l'objectif est de réaliser des activités d'audit interne et de scan de vulnérabilités périodique. En effet, un ensemble d'activités devront être prévus dans le cadre de la présente consultation. Ces activités vont être réalisées d'une manière périodique et itérative.

Ainsi, les activités à réaliser sont les suivantes :

- Audit interne du SMSI – incluant la vérification de la conformité du Système de Management de la Sécurité de l'Information du CRNS avec l'ISO 27001
- Audit de vulnérabilités et pentes du dispositif technique mis en place.

3. Tâches à réaliser et durée :

Ce projet d'assistance comporte 2 grandes phases. Un soumissionnaire doit soumettre pour toutes les phases.

Les différentes tâches ainsi que leurs durées respectives sont tracées dans le tableau suivant :

Phase	Description	Charge estimée
Phase 1 : Audit sécurité du SI	**1- Audit de conformité ISO27001 :2013 du Chapitre 4 à 10** **<u>Activités prévues :</u>** • Critères d'audit : conformité avec la norme ISO27001 :2013 du chapitre 4 à 10. • Revue documentaire • Entretiens et visites sur site	**10 H/ jours**
	2- Audit de conformité ISO27001 :2013 – Annexe A **<u>Activités prévues :</u>** • Critères d'audit : conformité avec la norme ISO27001 :2013 – Annexe A • Revue documentaire • Entretiens et visites sur site	**10 H/ jours**
	3- Post-Audit de conformité ISO27001 :2013 du Chapitre 4 à 10 A la suite de l'itération 1, les activités de post audit et de revue à prévoir : • Critères d'audit : conformité avec la norme ISO27001 :2013 – du chapitre 4 à 10 • Revue des améliorations apportées à la suite de l'audit itération 1	**5 H/ jours**
	4- Post-Audit de conformité ISO27001 :2013 – Annexe A A la suite de l'itération 2, les activités de post audit et de revue à prévoir : • Critères d'audit : conformité avec la norme ISO27001 :2013 – Annexe A • Revue des améliorations apportées à la suite de l'audit itération 2	**5 H/ jours**

Phase 2 : Mise en place d'un Dashboard de sécurité Technique	Le prestataire devrait s'engager à intégrer une solution permettant de fournir un moyen de surveillance du niveau de sécurité de l'entreprise à travers : • Une surveillance des événements de sécurité • La solution doit permettre d'intégrer un SIEM couvrant les composantes du SI • Permettant le suivi des logs et de présenter un Dashboard en temps réel des alertes de sécurité • Un suivi des vulnérabilités • Un Dashboard présentant le niveau de vulnérabilités et le niveau de conformité des composantes du SI au niveau des équipements de la CRNS La solution devrait être installé au niveau de : - 25 postes de travail - 1 Firewall - 03 serveurs	**5 H/ jours**
Phase 3 : Mission de Tests de vulnérabilités Périodiques	Le prestataire devrait s'engager à proposer deux missions de gestion de vulnérabilité incluant au minimum : – Revue de l'architecture réseau et des moyens de protection mis en place – Revue d'un échantillon de poste de travails, – Test et scan de vulnérabilités – Revue de vulnérabilité et de conformité sur un échantillon d'environnement de développement Les activités à réaliser pendant ces activités d'audit sont : • <u>Travaux de reconnaissance</u> – Reconnaissance externe – Reconnaissance interne – Reconnaissance des services exposés • <u>Identification de vulnérabilités techniques</u> – Revue de l'architecture réseau et des moyens de protection – Revue d'un échantillon de poste de travails – Test et scan de vulnérabilités internes incluant serveurs et applications – Revue de vulnérabilité et de conformité sur un échantillon d'environnement de développement • <u>Pentest</u> – Pentest interne et externe – Pentest d'un environnement projet (sur un échantillon d'environnement) De plus, l'ensemble des activités de revues techniques suivantes devraient être réalisé : • <u>Politique d'accès</u> – Accès AD – Accès aux environnements applicatifs – Accès aux environnements projets • <u>Politique de filtrage réseau</u> – Compartimentage réseau – Filtrage réseau	**10 H/ jours**

4. Qualification et profil (consultant, expert) :

- **Cabinet :**
  - Le cabinet doit être spécialisé en audit et conseil en sécurité de l'information
  - Avoir l'expérience professionnelle adéquate dans le domaine
- **Consultants proposés :**
  - Chef de projet :
    - Avoir l'expérience professionnelle nécessaire pour le bon déroulement de la mission.
    - Ayant une expérience significative dans l'implémentation ou suivi de processus ISO27001 : minimum 2 références
    - Certification : minimum requis
      - ✓ ISO27001 Lead Auditor
      - ✓ ISO27005 Risk Manager
      - ✓ Certifié sur une méthodologie d'analyse de risque (EBIOS, MEHARI,..)
  - 1 Membre de l'équipe :
    - Avoir l'expérience professionnelle nécessaire pour le bon déroulement de la mission
    - Certification : minimum requis
      - ✓ ISO27001 Lead Auditor ou bien ISO27005 Risk Manager

5. Pièces constitutives de la manifestation d'intérêt :

1- <u>Documents administratifs et techniques</u>

- Le présent cahier des charges signé avec la mention lue et approuvé
- Un certificat d'affiliation à un régime de sécurité sociale
- Un extrait du registre national des entreprises
- Fiche de renseignement général sur le soumissionnaire (selon le modèle ci-joint en annexe)
- Agrément
- Déclaration sur l'honneur de non influence (selon le modèle ci-joint en annexe)
- Déclaration sur l'honneur de non de non appartenance à l'administration qui va passer la consultation (selon le modèle ci-joint en annexe)
- Le planning d'exécution détaillé portant la signature du représentant légal de cabinet
- Copie des diplômes du chef d'équipe et du son assistant et des différentes pièces justificatives en termes d'expérience professionnelle.
- Référence récentes et pertinentes en missions similaires pour le cabinet.
- Preuves et qualifications en rapport avec la nature de la mission pour l'équipe projet.
- Curriculum Vitae des membres de l'équipe

2- <u>Documents financiers</u>

- La soumission signée par soumissionnaire.
- Le bordereau de prix

Les soumissions doivent parvenir par voie postale, ou doivent être déposées directement au bureau d'ordre du CRNS, à l'adresse ci-dessous, et ce au plus tard le **30/11/2023**, (le cachet du bureau d'ordre du centre faisant foi), avec la mention suivante : « **NE PAS OUVRIR » « Consultation N° 98/2023 – Audit de la sécurité du SMSI de Centre de Recherche en Numérique de Sfax »**

6. Conditions d'exécution de la mission :

- **Moyens et ressources à mobiliser par le cabinet :**

Le cabinet prend à sa charge les frais de transport : transport urbain et interurbain, l'hébergement et tous les frais engendrés par le séjour des personnes impliquées (Alimentation, ect..).
Il est tenu de mobiliser par ses soins les moyens logistiques primordiaux pour sa propre utilisation.

- **Données, service, locaux, personnel et Installations à fournir par le Centre durant la mission :**

Le Centre de Recherche s'engage à mettre à la disposition du cabinet, toutes les données nécessaires à l'exécution de sa mission et de mettre à sa disposition les équipements et les moyens matériels nécessaires durant l'exécution de la mission (Vidéoprojecteur, impression, tirage, support numérique, …).

- **Responsabilité du consultant :**

Le cabinet est censé s'acquitter de sa mission avec la diligence voulue et selon les règles de l'art.

7. Méthode de sélection

Sont admis à soumissionner les personnes morales capable d'honorer leurs engagements et présentant les garanties et les capacités nécessaires tant au plan professionnel que technique et financier mentionnées dans le présent appel à manifestation.

Une commission de sélection des candidatures établira un classement des candidatures selon l'offre financière, le soumissionnaire le moins disant sera examiné selon un barème de notation des qualifications techniques du cabinet et de l'équipe comme suit :

Critère	Barème	
Expérience du cabinet dans le domaine de la sécurité d'information	5<Expérience<10 ans	**10 points**
	Expérience>=10 ans	**20 points**
Nombre de missions similaires	< 3	**0 points**
	3<….<10	**10points**
	>= 10	**20 points**
Diplôme du chef d'équipe	Maitrise	**5 points**
	Ingénieur ou Mastère	**8 points**
	Doctorat	**10 points**
Expérience professionnelle du chef d'équipe	Entre 5 et 10 ans	**10 points**
	>= 10 ans	**20 points**
Nombre de missions similaires pour le chef d'équipe	Aucune mission	**0 points**
	<5 missions	**10 points**
	>= 5 missions	**20 points**
Expérience professionnelle de l'assistant	Entre 3 et 7 ans	**5 points**
	>= 7 ans	**10 points**

(*)Le dossier doit être appuyé par toutes les pièces justificatives.

La note technique minimale exigée est de 65 points. Tout cabinet ayant un score nul dans l'une des rubriques sera éliminé de la sélection, indépendamment de son score final.

Si la note technique obtenue dépasse 65 points, le candidat sera retenu pour la phase de négociation financière et technique, sinon il sera procédé de la même manière à l'évaluation technique du soumissionnaire suivant selon le classement financier.

Avant l'attribution définitive du contrat, celui-ci sera négocié avec le cabinet sélectionné.
Les sélections portent essentiellement sur :

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

8. Confidentialité :

Le cabinet 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. Il s'engage à ne pas utiliser ces données pour son propre compte ou pour le compte d'autrui. Tout manquement à cette clause entraine l'interruption immédiate de la mission.

Cette confidentialité reste en règle et sans limitation après la fin de la mission.

9. LIVRABLES

Le soumissionnaire doit livrer les documents suivants à la fin de la période d'exécution des différentes phases :

- Un Rapport d'audit SMSI de CRNS
- Un manuel d'utilisation de la solution de surveillance
- Un outil de surveillance
- Un / des rapports de test de vulnérabilité

10. ANNEXES

Annexe 01 : Fiche de renseignements généraux

Annexe 02 : SOUMISSION

Annexe 03 : Déclaration sur l'honneur de non-influence

Annexe 04 : Déclaration sur l'honneur de non-appartenance à l'administration qui va passer la consultation

Annexe 05 : Bordereau des prix

Consultation 98/2023

Audit de la sécurité du SMSI du Centre de Recherche en Numérique de Sfax

ANNEXE N°1

FICHE DE RENSEIGNEMENTS GENERAUX

SUR LE SOUMISSIONNAIRE

Nom et prénom/Dénomination sociale.....

Forme juridique.....

Adresse du siège.....

Téléphone.....Fax.....

Adresse……

email……

Inscrit au registre de commerce sous le n°……

N° du matricule fiscal.....

Fait à..... Le.....

Le soumissionnaire

(Cachet, nom et prénom, signature)

Consultation 98/2023

Audit de la sécurité du SMSI du Centre de Recherche en Numérique de Sfax

Annexe n°2
SOUMISSION

Je soussigné (Nom, prénom tels que figurant sur la CIN)……

Domicilié au …….. ……

Titulaire de la Carte d'Identité Nationale **N°**……délivrée le ……..

Exerçant la profession de ……

Adresse ……

……

Agissant en qualité de …….

Après avoir pris connaissance de toutes les pièces figurant ou indiquées au dossier de la consultation n° 98/2023, Je m'engage à exécuter les prestations conformément aux caractéristiques exigées dans le cahier des charges et moyennant les prix établis dans mon offre.

Les prix que j'offre sont fermes et non révisables.

Le montant total de cette soumission s'élève à la somme de …… (Montant en lettres et en chiffres **TTC**) ……

Je m'engage à maintenir valables les conditions de la présente soumission pendant **60** jours fermes à compter du jour suivant la date limite de réception des offres.

Je joins à la présente soumission toutes les pièces qu'il m'est demandé de fournir.

Je m'engage, si mon Offre est acceptée, à exécuter l'ensemble des prestations conformément aux termes des articles des conditions de participation, administratives et techniques du cahier des charges.

Fait à ……. Le ……..

Signature, date, nom et qualité du signataire

Consultation 98/2023

Audit de la sécurité du SMSI de Centre de Recherche en Numérique de Sfax

Annexe n°3

Déclaration sur l'honneur

(Concernant la confirmation de n' avoir pas fait et l'engagement de ne pas faire par lui-même ou par personne interposée des promesses, des dons ou des présents en vue d'influencer sur les différentes procédures de conclusion d'un marché et des étapes de sa réalisation)

Conformément au Décret N°2014-1039 du 13 Mars 2014 portant organisation des marchés publics;

Je soussigné,(1)……..

Agissant entant que (2)……..

De la Société (3)……

confirme de n'avoir pas fait et l'engagement de ne pas faire par moi-même ou par personne interposée des promesses, des dons ou des présents en vue d'influencer sur les différentes procédures de conclusion d'un marché et des étapes de sa réalisation

Fait à _____, le_____

Le soumissionnaire
(Nom et Prénom, Signature, Cachet et Qualité du Signataire)

(1) Nom et prénom du soumissionnaire.
(2) Qualité du soumissionnaire.
(3) Raison sociale de la société.

Consultation 98/2023
Audit de la sécurité du SMSI
de Centre de Recherche en Numérique de Sfax

Annexe n°4

Déclaration sur l'honneur de non appartenance à l'administration, l'établissement ou l'entreprise publique qui va passer la consultation

Conformément au décret N° 2014-1039 du 13 Mars 2014 portant organisation des marchés publics;

Je soussigné(1)……

Agissant en tant(2) ……

De la société (3) ……

Confirme que je n'étais pas un agent public au sein de l'administration qui va passer le marché dans le cadre de la consultation N° 98/2023 : Audit de la sécurité du SMSI de Centre de Recherche en Numérique de Sfax depuis au moins cinq ans.

Fait à _____ Le _____

Le soumissionnaire
(Nom et Prénoms, Qualité du signataire, Date et cachet)

_____

(1) Nom et prénom du soumissionnaire.

(2) Qualité du soumissionnaire.

(3) Raison sociale de la société.

Consultation 98/2023

Audit de la sécurité du SMSI de Centre de Recherche en Numérique de Sfax

Annexe n°5

Bordereau des prix

N°	Mission	Durée (Homme jour)	Prix Unitaire	Montant
01	**Audit de la sécurité du SMSI**	45 H/J (en présentiel)		
Total				

Fait à ……. Le ……..

Signature, date, nom et qualité du signataire