CAHIER DE CHARGES
POUR L'AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION DE LA FNARC

Consultation N°6 2014

Juin 2014

CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIERES

Article 1 : Objet de la consultation

La Fondation Nationale d'Amélioration de la Race Chevaline (FNARC) se propose de lancer une **consultation** 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.

Article 2: Conditions de participation

Cette consultation s'adresse aux entreprises **certifiées par l'Agence Nationale de la Sécurité Informatique conformément au décret N° 1249-2004 du 25 mai 2004**.

Article 3 : Présentation de l'offre

Les soumissionnaires devront faire parvenir leurs offres et pièces annexes au plus tard le **04 Juillet 2014 à 12 heures au siège de la FNARC**, par voie postale ou par rapide poste ou directement au bureau d'ordre de la FNARC, 2020 Sidi Thabet BP 61 , Tunis.

Les offres doivent être présentées, comme suit :

Une enveloppe extérieure fermée, libellée au nom de Monsieur le Directeur Général de la FNARC, portant la mention :

«A NE PAS OUVRIR –
CONSULTATION N° 6 2014
POUR AUDIT DE LA SECURITE
DU SYSTEME D'INFORMATION DE LA FNARC»

Cette enveloppe comportera :

Une enveloppe A : comportant les pièces administratives et techniques

A.1 Les pièces administratives

1- Le cahier des clauses administratives avec signature et cachet du soumissionnaire au bas de chaque page .La mention «lu et approuvé » doit être inscrite sur la dernière page

2- Attestation d'affiliation à la Caisse Nationale de la Sécurité Sociale du soumissionnaire valable à la date limite de dépôt des offres. (original ou copie conforme)

3- Une copie conforme du certificat ANSI du soumissionnaire certifié en cours de validité

4- Les copies conformes des certificats ANSI des auditeurs certifiés (membres de l'équipe intervenante), en cours de validité

5- Une déclaration sur l'honneur de non faillite

6- Une déclaration sur l'honneur de non influence sur les différentes procédures de conclusions de cette mission.

7- Une déclaration sur l'honneur de non appartenance à la Fondation Nationale d'Amélioration de la Race Chevaline.

8- Une caution provisoire établie conformément au modèle ci-joint en annexe 6

9- Attestation fiscale prévue par la législation en vigueur valable le jour de l'ouverture des plis

A.2- Le dossier technique : le dossier technique doit comporter les pièces suivantes :

1- Le cahier des clauses techniques avec signature et cachet du soumissionnaire au bas de chaque page .La mention «lu et approuvé » doit être inscrite sur la dernière page

2- Un aperçu succinct sur l'activité générale du bureau du soumissionnaire, son organisation et son expérience dans le domaine de sécurité.

3- Présentation des références du soumissionnaire

4- Méthodologie(s) proposée(s) pour la conduite du volet audit organisationnel, physique et technique incluant la spécification des outils et scripts à utiliser

5- Le planning prévisionnel d'exécution, spécifiant clairement toutes les phases d'exécution, accompagné des modèles de l'Annexe 2 y afférents, remplis, avec précision.

6- Les CVs et références de l'équipe d'audit proposée

Toutes les pages des documents exigés dans le dossier technique doivent être datées, signées et comporter le cachet du soumissionnaire.

Enveloppe B : Le dossier financier qui doit comporter :

- La Soumission selon modèle en annexe 4
- Le Bordereau des prix rempli et signé (Annexe 5)

Toutes les pages des documents exigés dans le dossier financier doivent être datées, signées et comporter le cachet du soumissionnaire.

Toute offre parvenue après le délai sera rejetée, le cachet du bureau d'ordre de la FNARC fait foi.

Article 4 : Langue de l'offre

L'offre préparée par le soumissionnaire les caractéristiques techniques et tout document concernant l'offre, échangé entre le soumissionnaire et la FNARC devront être rédigés en langue française.

ARTICLE 5: DUREE DE VALIDITE DES OFFRES

La durée de validité des offres est fixée à 90 jours, de la date limite de dépôt des offres.
La FNARC se réserve le droit de ne donner aucune suite aux propositions reçues.

ARTICLE 6: NATURE DES PRIX

Les prix offerts par le soumissionnaire sont fermes et non révisables pendant toute la durée d'exécution du marché.

Article 7 : Durée de réalisation de la mission

La durée de réalisation de la mission objet du présent cahier des charges, ne doit pas dépasser trente (30) jours ouvrables.

Le délai de finalisation de la mission devra être égal à la durée spécifiée dans le planning proposé dans l'offre, à moins d'un accord contraire établi lors de la phase préliminaire de démarrage.

Ce délai ne tient pas compte des délais additionnels éventuels pris pour la correction (validation) des différents livrables exigés dans le présent cahier des charges, et ce conformément à l'article 08 « Réception » et des délais d'évaluation du rapport par l'ANSI.

Article 8 : Réception

La FNARC appliquera deux phases de réception :

1- Première phase :

Cette phase consiste en l'approbation par la FNARC du rapport préliminaire d'audit de la structure auditée portant le cachet et la signature du Titulaire.

Ce rapport d'audit doit comprendre au minimum les quatre 04 sections 1.a), 1.b), 1.c) et 1.d) spécifiées par l'article 4 : livrables, du Cahier des Clauses Techniques Particulières.

Le chef de Projet de la FNARC donnera son avis quant à la consistance et la pertinence du rapport, en regard :

- de la qualité de réalisation des objectifs assignés à la mission et fixés dans le Cahier des Clauses Techniques et, le cas échéant, tels que raffinés lors de la phase de démarrage,
- de l'adéquation de la méthodologie mise en œuvre par le titulaire lors de la réalisation de la mission, avec celle consignée dans son offre,

- de la qualité des résultats (estimation des risques, ...) issus des travaux d'audit et de leur complétude,
- de la qualité des recommandations émises,
- et le cas échéant, de la qualité des mesures d'accompagnement consignées.

2- Deuxième phase :

Cette phase consiste en la soumission du rapport final d'audit portant le cachet et la signature du titulaire à l'approbation de la FNARC.

Ce rapport devra être remis par le titulaire dans les délais impartis (en tenant compte de l'éventuel rallongement induit par la première phase. Tout retard imputé au titulaire donnera lieu à l'application de la clause de pénalité du présent Cahier des Charges.

Le chef de Projet de la FNARC donnera son avis quant à la consistance et la pertinence du rapport, en regard (en sus des critères fixés dans la précédente phase) :

- de la qualité et complétude des livrables fournis,
- de la qualité (pertinence, pragmatisme) des recommandations issues des travaux d'audit et de leur complétude,
- de la qualité du plan d'action opérationnel et du plan d'action cadre s'étalant sur trois ans.

Pour toutes les phases de réception, la FNARC se chargera de communiquer son avis quant à la consistance et la pertinence du rapport au titulaire dans un délai ne dépassant pas quinze (15) Jours ouvrables à partir de la date de réception du rapport. Dépassé ce délai, ledit rapport sera considéré comme validé.

Au cas où l'avis consigne des réserves, le titulaire devra les lever dans une période ne dépassant pas dix (10) jours ouvrables à partir de la date de leur notification, sauf accord contraire entre les deux parties, compte tenu du volume des corrections. Ces réserves devront être insérées dans le rapport final de l'audit au sein d'une annexe « PVs et Correspondances ».

En cas de conflit insoluble et après avoir entamé toutes les procédures de rapprochement nécessaire, la FNARC et éventuellement le titulaire pourraient demander l'arbitrage de l'ANSI ou de la commission d'arbitrage énoncée dans la réglementation des marchés publics ou d'un expert certifié conformément au décret 2004-1249 du 25 mai 2004, accepté par les deux parties et ce pour décider de la suite à donner à ce conflit, avant d'intenter une procédure de résiliation et éventuellement pénale.

Article 9 : Missions de reconnaissance

En vue de l'élaboration de leurs offres, les soumissionnaires pourraient entreprendre, à leurs frais, des missions préalables de reconnaissance, auprès des structures à auditer. Ils devront présenter une demande écrite à la FNARC. Cette visite sera organisée, en commun pour tous ceux qui en ont fait la requête ou manifesté par écrit leur souhait d'y participer au moins dix (10) jours ouvrables avant la date de remise des offres, via une notification écrite à tous les concernés. Les visiteurs devront :

- faire partie du personnel permanent du soumissionnaire,
- être astreints à la confidentialité et être auditeurs certifiés par l'ANSI.

Ils devront de plus, ramener une attestation de respect total de la confidentialité attribuée à cette opération de reconnaissance (annexes 3), cosignée par le visiteur et le responsable du soumissionnaire qui l'aura affecté à cette mission.

ARTICLE 10 - CAUTIONS

A-CAUTION PROVISOIRE :

Le soumissionnaire doit fournir un cautionnement provisoire égal à **100** DT
La caution, d'une validité de 90 jours, restera obligatoirement valable jusqu'au jour de son remplacement par une caution définitive. Néanmoins, elle sera restituée, aux soumissionnaires non retenus, après le résultat officiel de la dite consultation.

B-CAUTION DEFINITIVE :

Le montant de la caution définitif est fixé à 3% (trois pour cent) du montant du marché en TTC, augmenté le cas échéant des montants des avenants.
Le cautionnement devra être constitué dans un délai de vingt (20) jours, à partir de la date de la notification de l'approbation du marché par des cautions personnelles et solidaires établies conformément à la règlementation en vigueur.
Le cautionnement définitif est restitué ou la caution qui le remplace libérée si le titulaire du marché s'est acquitté de ses obligations dans un délai d'un mois à compter de la date de réception définitive.

La caution cesse d'avoir effet à l'expiration des délais visés ci-dessus, sauf si la Fondation Nationale d'Amélioration de la Race Chevaline a signalé par lettre recommandée avec accusé de réception adressée à la banque que le titulaire n'a pas rempli toutes ses obligations.
Dans ce cas il ne peut être mis fin à l'engagement de la caution que par mainlevée délivrée par la personne responsable du marché.

Article 11 : Pénalités de retard

Si les délais prévus par le marché ne sont pas respectés par le titulaire celui-ci sera passible d'une pénalité calculée à raison de 1/1000 pour chaque jour de retard sur la

valeur de la phase de la mission objet du retard, sans qu'une mise en demeure préalable ne soit nécessaire. Le montant de la pénalité ne dépassera pas 5% du montant de la phase de la mission. Ces dispositions sont appliquées chaque fois qu'un retard est manifesté dans l'exécution d'une phase de la mission et auront un effet cumulatif.

Article 12 : Secret professionnel

Le titulaire s'engage à ne pas rendre public ou divulguer à qui que ce soit sous forme écrite, orale, ou électronique les résultats de l'audit ou toute information relevant de la structure auditée et à laquelle il a eu accès dans l'exécution de sa mission ou pour la soumission de son offre. La FNARC interdit aux soumissionnaires et au titulaire de délivrer via n'importe quel moyen de communication, toute information confidentielle relative au Système d'Information et spécialement toute information pouvant :

- Donner une indication sur l'architecture réseau, la configuration matérielle ou logicielle, les plates-formes, les serveurs, etc... et toute composante des systèmes d'information et de communication.

- Donner une indication sur les mécanismes de contrôle d'accès et de protection du système d'information et des dispositifs de sécurité physique ou logique.

- Donner une indication sur la politique sécuritaire, les programmes présents ou à venir, les budgets, ou toute autre information relevant des affaires internes de l'organisation auditée.

- Donner une indication sur tout type de faille organisationnelle ou technique décelée.

Et d'une façon générale, le titulaire est tenu au secret professionnel et à l'obligation de discrétion pour tout ce qui concerne les faits, informations, études et décisions dont il aura eu connaissance au cours de l'exécution du présent marché ou pour la soumission de son offre ; il s'interdit notamment toute communication écrite, électronique ou verbale sur ces sujets et toute remise de documents à des tiers.

Article 13 : Entrée en vigueur

L'entrée en vigueur de la mission d'audit aura lieu suite à la réception du bon de commande par le titulaire.

Article 14 : Validation par l'ANSI

Le rapport final ainsi que tous les procès-verbaux et le planning réel d'exécution de la mission doivent être remis à l'Agence Nationale de la Sécurité Informatique conformément aux dispositions du décret 1250-2004.
Si le rapport d'audit sera refusé par l'Agence Nationale de Sécurité Informatique, pour manquement grave aux prescriptions du décret 1250-2004, le titulaire est tenu de procéder à ses frais, à la correction des manques signalés .

Article 15 : Modalités de paiement

Le paiement de la mission d'audit objet de cette consultation s'effectuera comme suit :

- **20 %** du côut total à la **commande**

- **40 %** à la réception et la **validation du rapport préliminaire** d'audit (phase 1 de l'article 08 du cahier des clauses administratives particulières)

- **40 %** à la réception et **validation du rapport final** d'audit par la FNARC (phase 2 de l'article 08 du cahier des clauses administratives particulières) et suite **à l'avis favorable de l'Agence Nationale de la Sécurité Informatique.**

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

Article 1 : Objet de la consultation

La mission objet de cette consultation concerne l'audit de la sécurité du système d'information de la FNARC décrit dans l'annexe 1.

L'objet de cet audit devra se conformer, au minimum, aux dispositions énoncées dans le décret N°2004-1250 du 25 mai 2004 et être réalisé par une entreprise certifiée par l'ANSI conformément au décret N° 2004-1249 du 25 mai 2004.

Cet audit devra prendre comme référentiel de base la norme ISO/IEC 27002 et suivre une approche méthodologique aussi proche que possible de ce référentiel.

La mission d'audit objet de cette consultation devra ainsi concerner les aspects organisationnels, physiques et techniques, relatifs à la sécurité du Système d'Information inclus dans le périmètre de cet audit.

Article 2 : Conduite et déroulement de la mission

Cette mission sera décomposée en quatre phases principales listées selon les conseils relatifs à la planification et à la réalisation des activités d'audit donnés dans la norme ISO 19011 :

I- Déclenchement de la mission d'audit :

Au lancement de l'audit, le titulaire devra solliciter auprès des structures à auditer tout détail, information ou document nécessaire pour l'exercice de sa mission.

Une réunion préparatoire de la mission sera organisée au début de la mission, dont l'objet sera de finaliser, sur la base des besoins et documents préparés par le titulaire, les détails de mise en œuvre de la mission.

Il concernera, sans s'y limiter, la finalisation des détails suivants :

- désignation des chefs de projets et des interlocuteurs, côtés FNARC et titulaire,
- validation du périmètre de l'audit,
- fourniture des documents requis pour l'audit (manuels d'exploitation, schémas d'architectures, politique de sécurité, …),
- fourniture du document de définition des besoins de sécurité. Si ce document n'existe pas, la FNARC tâchera à le préparer et le fournira au titulaire avant le démarrage de l'audit sur site,
- examen des détails des listes des interviews à réaliser par le titulaire et fourniture par la FNARC de la liste nominative des personnes à interviewer,

- affinement des plannings d'exécution (planning des actions par site, plannings des réunions de coordination et de synthèse, ….),
- examen des détails logistiques nécessaires au déroulement de la mission (octroi des autorisations d'accès aux lieux où l'audit devra être élaboré sur la base d'études de terrain, octroi de locaux de travail au titulaire,…).

Ainsi tous les détails de mise en œuvre seront examinés et validés. Cette réunion débouchera, entre autre, sur la synthèse des plannings précis et détaillés de mise en œuvre de la mission.

Les résultats de cette réunion seront consignés dans un PV, qui sera annexé au rapport final d'audit.

II- Phase de sensibilisation

Des sessions de sensibilisation préliminaires, destinées aux responsables et acteurs du système d'information, devront être proposées.

Ces sessions préliminaires auront pour premier objectif une sensibilisation générale sur les dangers cybernétiques et sur les risques cachés encourus, incluant entre autres la présentation pratique d'attaques cybernétiques. Elles devront aussi rappeler les objectifs de l'audit, l'urgence et les bienfaits attendus, ainsi que l'assurance sur la confidentialité des données reçues.

A la fin de cette opération un PV sera dressé et signé conjointement par le titulaire et la FNARC et sera joint au rapport d'audit.

Le soumissionnaire devrait indiquer dans son offre, le nombre de sessions de sensibilisation préliminaires à réaliser.

III- Conduite des activités d'audit :

C'est la phase d'audit proprement dite.

Ainsi, cette phase couvrira principalement trois (03) volets :

- un volet d'audit organisationnel et physique,
- un volet d'audit technique,
- et un volet d'appréciation des risques.

A. Audit organisationnel et physique :

Il s'agit, pour ce volet, d'évaluer les aspects organisationnels de gestion de la sécurité des structures objet de l'audit. Au cours de cette étape, le titulaire devra emprunter une approche méthodologique, basée sur des batteries de questionnaires pré-établis et adaptés à la réalité des entités auditées et aux résultats de la revue des documents. Cette approche permettra d'aboutir à une évaluation pragmatique des

failles et des risques encourus et de déduire les recommandations adéquates pour la mise en place des mesures organisationnelles et d'une politique sécuritaire adéquate.

Cet audit devra prendre comme référentiel tous les chapitres de la dernière version de la norme ISO/IEC 27002.

B. Audit technique :

1. Objectifs de l'audit technique

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. 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. Ces tests doivent englober des opérations de simulation d'intrusions et tout autre test 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 titulaire 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 mises en œuvre.
- évaluer la vulnérabilité et la 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'attaques 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, ..)

- évaluer l'herméticité des frontières du réseau contre les tentatives de son exploitation par des attaquants externes
- Il 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 FNARC). Ils 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.

2. Outils de l'audit technique

Les outils proposés devront inclure, sans s'y limiter, les catégories d'outils suivants :

- outils de sondage et de reconnaissance du réseau,
- outils de test automatique de vulnérabilités du réseau,
- outils spécialisés dans l'audit des équipements réseau (routeurs, switchs, …),
- outils spécialisés dans l'audit de chaque type de plate-forme système (OS, ..) présente dans l'infrastructure,
- outils spécialisés dans l'audit des SGBD existants,
- outils de test de la solidité des objets d'authentification (fichiers de mots clés, …),
- outils d'analyse et d'interception de flux réseaux,
- outils de test de la solidité des outils de sécurité réseau (firewalls, IDS, outils d'authentification,….),

et tout autre type d'outil, recensé nécessaire, relativement aux spécificités du système d'information audité.

C. Appréciation des risques :

Dans ce volet 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.

Le volet d'appréciation des risques se déroulera en deux étapes :

Etape 1 : Analyse

A cette étape le titulaire est amené à :

1. identifier les **processus critiques** : les informations **traitées**, les actifs matériels, les actifs logiciels, les personnels,…qui supportent ces processus,
2. identifier les **menaces** auxquelles sont confrontés ces actifs (intentionnelles ou non intentionnelles),
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. évaluer la **probabilité** réaliste d'une défaillance de sécurité au vu des mesures actuellement mises en œuvre.

Etape 2 : Evaluation

A cette étape le titulaire est amené à :

1- établir une classification des risques par niveaux, et déterminer le niveau du risque acceptable,

2- évaluer 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.

IV-Préparation du rapport d'audit :

Le titulaire est invité, à la fin de la phase d'audit sur terrain, à remettre à la FNARC un rapport daté, signé par le responsable de l'audit et portant le cachet du titulaire.

Ce rapport doit contenir 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 :

1. les actions détaillées (organisationnelles et techniques) urgentes à mettre en œuvre dans l'immédiat, pour parer aux défaillances les plus graves, ainsi que la proposition de la mise à jour ou de l'élaboration de la politique de sécurité à instaurer,
2. 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 à intenter, procédures d'exploitation sécurisées à instaurer,…) et technique (outils et mécanismes de sécurité à mettre en œuvre), ainsi qu'éventuellement des aménagements architecturaux de la solution de sécurité existante,
- une estimation des formations requises et des ressources humaines et financières supplémentaires nécessitées.

3. la proposition d'un plan d'action cadre s'étalant sur trois années et présentant un planning des mesures stratégiques en matière de sécurité à entreprendre, et d'une manière indicative les moyens humains et financiers à allouer pour réaliser cette stratégie.

Article 3 : Méthodologie(s) adoptée(s)

Pour la réalisation de la mission, le soumissionnaire devra emprunter une approche méthodologique, en indiquant les références de la (ou des) méthodologie(s) adoptée(s), tout en gardant comme référentiel normatif la norme ISO/IEC 27002.

La (les) méthodologie(s) adoptée(s) devra(ont) être adaptée(s), dans sa (leur) mise en œuvre, à la réalité métier et à la taille des entités auditées et devra(ont) permettre d'aboutir à l'élaboration de bilans et de recommandations et des solutions pragmatiques et pertinentes, qui tiennent compte, pour les plus urgentes, de la réalité humaine et matérielle de l'entité, et en la corrélant à la gravité des failles décelées et à l'efficacité, l'urgence et la faisabilité des actions à mener .

Ainsi, le soumissionnaire est appelé à indiquer, clairement dans son offre, la (les) méthodologie(s) d'audit qu'il envisage de mettre en œuvre, tout en fournissant des références sur son adéquation avec le référentiel ISO/IEC 27002. La FNARC tiendra compte dans son évaluation de la consistance de la (des) méthodologie(s) proposée(s), ou parties de cette (ces) méthodologie(s) et ce à chaque phase ainsi que de son (leur) adéquation à la réalité de l'entreprise et du temps imparti.

Il devra aussi indiquer dans son offre la qualité des moyens techniques et humains qui seront déployés lors de la mise en œuvre de cette (ces) méthodologie(s) (expérience dans la mise en œuvre de la (des) méthodologie(s) consignée(s), outils logiciels accompagnant la mise en œuvre de cette (ces) méthodologie(s)).

Le soumissionnaire devra spécifier dans la rubrique « Démarche d'audit proposée », au minimum, et pour chaque composante du système d'information :

- le Type de méthodologie(s) à mettre en œuvre pour le volet physique et organisationnel et les structures recensées utiles à interviewer, ainsi que l'(es) outil(s) logiciel(s) accompagnant la mise en œuvre de cette (ces) méthodologie(s) (traitement automatisé des interviews et calcul des risques associés, …),
- la méthode de mise en œuvre du volet technique, en spécifiant les types de tests techniques à effectuer et leurs objectifs, ainsi que les outils utilisés,
- la séquence des actions à mener (interviews, tests techniques, synthèse, rédaction de rapports, …) et une estimation de la volumétrie homme/jour de chaque action
- la liste nominative des équipes qui interviendront pour chaque composante (site, structure) avec référence de l'expérience dans la mise en œuvre de la (des) méthodologie(s) et des outils consignés.

Il est à noter que toute modification des personnes initialement proposées est une cause de rupture du contrat ou de disqualification, sauf cas exceptionnel, via l'octroi de l'accord préalable et écrit de la FNARC (avec insertion de ces écrits dans le rapport final). De plus, le personnel en charge de l'audit devra être un personnel permanent du soumissionnaire. Pour autant, le soumissionnaire pourrait éventuellement faire intervenir du personnel consultant, sur la foi de présentation du contrat de consultation y afférant, qui devrait inclure une clause sur la confidentialité, tout en assumant totalement la responsabilité envers tout risque de divulgation par ce personnel de tout type de renseignements concernant cet audit.

Article 4 : Livrables

Le rapport d'audit devra couvrir, au minimum, les aspects mentionnés dans le décret N°2004-1250 du 25 mai 2004.

Le document final devra inclure les chapitres ou rapports suivants :

1. Description du système d'information de l'organisme
2. Un rapport détaillé d'audit couvrant les différents aspects spécifiés dans le Cahier des Clauses Techniques et comprenant au minimum les sections suivantes :

    a) une section relative à l'audit organisationnel et physique, fournissant l'ensemble des failles d'ordre organisationnel et physique et incluant la liste des recommandations à appliquer dans l'immédiat, en tenant compte des spécificités de l'entité, de la classification des systèmes (criticité) et de la réalité actuelle des moyens humains et financiers,

b) une section relative à l'audit technique, indiquant les vulnérabilités existantes, leur impact sur la pérennité des systèmes d'information et de communication de la structure, en incluant des recommandations techniques à appliquer dans l'immédiat, concernant les moyens (réalistes) de correction des failles graves décelées. Tous les travaux de test et d'analyse effectués devront être consignés dans une annexe, en les ordonnant selon leur sévérité, en incluant au niveau du rapport un relevé des failles les plus importantes et des moyens de les combler dans l'immédiat,

c) une section relative à la partie analyse des risques fournissant une évaluation des risques résultant des menaces identifiées et des failles découvertes lors des phases d'audit organisationnel, physique et technique,

d) une section relative au plan d'action et à la stratégie de sécurité à appliquer sur le court terme (jusqu'au prochain audit). Cette section comprendra des recommandations précises quant aux mesures à prendre dans le court terme, afin de pallier aux failles et insuffisances décelées. Elle inclura tous les nécessaires organisationnels et techniques en tenant compte, pour ce qui concerne le déploiement d'outils et d'architectures de sécurité, de l'option d'usage d'outils open-source et de la réalité financière et humaine de l'entité.

3. un rapport présentant le plan d'action cadre s'étalant sur trois années, permettant de mettre en œuvre une stratégie de sécurité cohérente et ciblée. Ce rapport sera mis à jour lors des audits de la seconde et de la troisième année tenant compte du taux de réalisation des mesures qui ont été adoptées depuis le dernier audit réalisé et des insuffisances enregistrées dans l'application de ses recommandations, ainsi que des résultats de l'audit de l'année en cours,
4. un rapport de synthèse, destiné à la direction générale (destiné décideurs), qui inclura d'une manière claire les importants résultats de l'estimation des risques, un résumé succinct des importantes mesures organisationnelles, physiques et techniques préconisées dans l'immédiat et sur le moyen terme (jusqu'au prochain audit), ainsi que les grandes lignes du plan d'action cadre proposé,

METHODOLOGIE DE DEPOUILLEMENT

Article 1er : Critères de conformité technique

Il sera tenu compte lors de l'évaluation technique des offres, des compétences et de la qualification de l'équipe d'audit et de la méthodologie d'audit.

Les critères de conformité technique sont :

1. le soumissionnaire est certifié par l'Agence Nationale de la Sécurité Informatique, conformément au décret N° 2004-1249 du 25 mai 2004, en cours de validité,
2. le chef du projet est un auditeur certifié par l'Agence Nationale de la Sécurité Informatique, conformément au décret susmentionné, en cours de validité,
3. le nombre d'intervenants est de deux [2] personnes au minimum, sans compter le chef de projet,
4. l'expérience du chef de projet est supérieure ou égale à 5 ans,
5. le chef de projet doit avoir piloté au moins 3 missions d'audit de sécurité des systèmes d'information,
6. l'expérience de chaque membre de l'équipe intervenante est supérieure ou égale à 5 ans,
7. chaque membre de l'équipe intervenante doit avoir participé à au moins 3 missions d'audit de sécurité des systèmes d'information .
8. présentation de la méthodologie de conduite du projet tout en fournissant des références sur son adéquation avec le référentiel ISO IEC 27002.

Article 2 : Critères d'évaluation

Le soumissionnaire sera retenu sur la base des critères suivants :

- **Critères techniques** : toute offre **ne répondant pas** à l'un des critères d'élimination (Article 1er : critère de conformité technique) **sera éliminée**,
- **Critères financiers** : l'offre la moins disante sera retenue.

ANNEXES

1- Structures à auditer et description du Système Informatique de la FNARC

2- Planning prévisionnel d'exécution

3- Déclarations sur l'honneur de confidentialité du soumissionnaire et des auditeurs (délégués)

4- Modèle de soumission

5- Bordereau des prix

6- Modèle de Caution Provisoire

ANNEXE 1

Structures à auditer

Description du Système Informatique

de la ***FNARC***

Structure	Lieu d'implantation (gouvernorat)
Siège de la FNARC	Situé à 2020 Sidi Thabet, Gouvernorat de l'Ariana Tunis

I- Réseaux et Equipements

Equipement	Nombre	Type / Marque	Observations
Réseaux locaux	**2**	**Câblage**	**Connectés par antennes dans 2 batiments distants**
Switchs	**2**	**- EDIMAX** **- D-Link**	**16 ports** **16 ports**
Modems	**1**	**SAGEM**	
Connexions Internet	**1**	**ADSL**	**4 M**

II- Matériel

1- Serveurs

Marque	Caractéristiques	Quantité	Système d'exploitation	SGBD	Année d'acquisition	Nombre de postes connectés
Dell Power Edge 840	Intel Xeon 2,13 Ghz RAM : 2Go	1	Windows Server 2003 SBS	SQL Server 2005	2009	11
Dell Power Edge T420	Intel Xeon RAM : 12 Go	1	Windows Server 2008 R2	Oracle 11 g	2014	10
NEC Express 5800	Intel Xeon 3,06 Ghz RAM : 1Go	1	Windows Server 2003	Oracle 10g	2004	0

2-Ordinateurs de bureau

25 Ordinateurs:

- 13 ordinateurs au niveau de la Direction Administrative et Financière et

- 12 ordinateurs au niveau de la Direction Technique

Description des ordinateurs de la Direction Administrative et Financière

Marque	Quantité	S.Exploitaion	Année d'acquisition	Connexion au réseau oui / non
HP Pro 3010	**4**	Windows 7	2010	Oui
HP Pro 3400	**4**	Windows 7	2012	Oui

COMPAQ	**1**	Windows 98	2001	Non
NEC PIV	**1**	Windows XP	2006	Oui
HP Pro 3500	**1**	Windows 7	2013	Oui
HP Pro 3130	**2**	Windows 7	2011	Oui
Total	**13**			**12 postes connectés au réseau**

Description des ordinateurs de la Direction Technique

Marque	**Quantité**	**S.Exploitaion**	**Année d'acquisition**	**Connexion au réseau** Oui / Non
HP Pro 3120	2	Windows 7	2010	Oui
NEC PIV	1	Windows XP	2003	Oui
NEC PIV	1	Windows XP	2005	Oui
HP Pro 3130	2	Windows 7	2011	Oui
NEC PIV	2	Windows XP	2004	Oui
HP Pro 3010	3	Windows XP	2010	Oui
HP Pro 3400	1	Windows 7	2012	Oui
Total	**12**			**12 Postes connectés au réseau**

III- Applications et Logiciels installés

Application	Description	Nombre d'utilisateurs	Type
OPENPGI	**Gestion Financière et Comptable**	**6**	**réseau**
OUJOUR	**Gestion de la Paie**	**1**	**monoposte**
SIRE	**Gestion des Chevaux**	**15**	**réseau**
ABSORDRE	**Gestion de Bureau d'Ordre**	**1**	**monoposte**
MAYAR	**Gestion de Stock**	**2**	**Réseau**
WADHIFA	**Gestion de personnel**	**4**	**Réseau**

IV- Antivirus installés :

Antivirus libres : Nod 32 Microsoft Security Essentials, Avast, Avira, …etc

ANNEXE 2

Planning prévisionnel de la mission

26Composant		Equipe intervenante	Durée en Hommes/jours pour chaque intervenant		Logistique utilisée (Outils,…)	Livrable
Phase	**Objet de la sous phase**		**Sur Site**	**Totale**		
Audit Organisationnel et physique	1: ……...	Nom:……				
	2: ……	Nom:……				
	….	Nom:……				
	n: ……	Nom:……				
Audit Technique	1: ……...	Nom:……				
	2: ……	Nom:……				
	….	Nom:……				
	n: ……	Nom:……				
Volet Sensibilisation	1: ……...	Nom:……				
	2: ……	Nom:……				
	…	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 3.1

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE
(Soumissionnaire)

Je soussigné Mr……., Responsable de la société …… déclare désigner

Mr …….. 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 préparatoire à la soumission de notre offre pour le marché ……. de la société ……

Le Soumissionnaire

(Cachet et signature)

ANNEXE 3.2

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE
(Soumissionnaire)

Je soussigné Mr ……., Responsable de la société ……. déclare désigner Mr …….. Expert auditeur, certifié par l'Agence Nationale de la Sécurité Informatique et faisant partie de notre société, pour nous représenter dans la visite sur terrain, préparatoire à la soumission de notre offre pour le marché …….. de la société ……

Le Soumissionnaire

(Cachet et signature)

ANNEXE 3.3

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE
(Délégué)

Je soussigné Mr ……., expert auditeur , certifié par l'Agence Nationale de la Sécurité Informatique et faisant partie de la société ……, déclare sur l'honneur maintenir une confidentialité totale sur toute information ou indication obtenue lors de la réunion d'éclaircissement préparatoire à la soumission de l'offre de la société ……que je représente et organisée par le maître d'ouvrage …….

Mr ……..,

CIN N° ……..

(Cachet de la société et signature)

ANNEXE 3.4

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE
(Délégué)

Je soussigné Mr ……., expert auditeur , certifié par l'Agence Nationale de la Sécurité Informatique et faisant partie de la société ……, déclare sur l'honneur maintenir une confidentialité totale sur toute information ou indication obtenue lors de la visite sur terrain, préparatoire à la soumission de l'offre de la société ……..…que je représente et organisée par le maître d'ouvrage ……..…….

Mr ……..,

CIN N° ……..

(Cachet de la société et signature)

Annexe 4

MODELE DE SOUMISSION

Je soussigné …… ……
(Nom, Prénom, Profession)
…….
Faisant élection de domicile au ……..

Agissant en qualité de……...
de la société …...……..….
(Nom et type de société)
Inscrit au registre de commerce de……
Sous le numéro dont le siège est à
…….
(Adresse complete)……
……..

Me soumets et m'engage à exécuter la mission d'audit du système d'information de la FNARC conformément aux conditions du cahier des charges - dont j'ai arrêté le montant à la somme de :
(en toutes lettres) ……
……
Se détaillant comme suit (en chiffres) :
Montant H T :…….

T.V.A :……

Montant T.T.C :……

Fait à le,

Signature et Cachet du soumissionnaire

Annexe 5

MODELE DE BORDEREAU DES PRIX

Soumissionnaire :……..

Désignation	Nombre d'hommes/jours	P.U. HTVA	P.T HTVA	Taux de la TVA	Montant de la TVA	P.T TTC
Audit organisationnel et physique						
Audit technique						
Rapport final						
Total						

Annexe : 6

MODELE DE CAUTION PROVISOIRE

Je soussigné – nous soussignés (1) ……..
…… agissant en qualité de ……de (2) ……..……..…….……..

1) certifie – certifions que ……..…..…… a été agrée par le Ministre des finances en application du décret n° 2002-3158 du 17 décembre 2002, portant réglementation des marchés public, que cet agrément n'a pas été révoqué, que (3) ……..……. a constitué entre les mains du trésorier général de Tunisie suivant récépissé n° …….. en date du …… la caution fixe de 5000 dinars prévu par le décret susvisé et que cette caution n'a pas été restitué.

2) Déclare me – déclarons nous, porter caution personnelle et solidaire (4) ……
…….domicilié à (5) …….
……..…… pour le montant de la retenue de garantie, auxquels ce dernier est assujetti en qualité de soumissionnaire de l'appel d'offre de la Fondation Nationale d'Amélioration de la Race Chevaline n° 01/2012 INF concernant la mission décrite dans le cahier des clauses techniques ci-joint.

Le montant de la dite caution s'élève à ……..dinars (6).

3) M'engage – nous engageons à effectuer le versement des sommes susvisées et dont le titulaire serait débiteur au titre du marché, et ce à la première demande écrite de la Fondation Nationale d'Amélioration de la Race Chevaline sans qu'il y ait besoin d'une mise en demeure ou d'une démarche administrative ou juridique quelconque.

la caution provisoire est libérée une fois le titulaire provisoire de la caution définitive.

La présente caution sera valable quatre vingt dix (120) jours à partir de la date des remises des offres.

---

(1) Noms et Prénoms du ou des signataires
(2) Raison Sociale et adresse de l'établissement garant
(3) Raison sociale de l'établissement garant
(4) Nom du soumissionnaire
(5) Adresse du soumissionnaire
(6) Le montant en toutes lettres.