REPUBLIQUE TUNISIENNE

***

MINISTÈRE DES AFFAIRES LOCALES ET DE L'ENVIRONNEMENT

***

AGENCE DE PROTECTION ET D'AMÉNAGEMENT DU LITTORAL

A.P.A.L.

APAL

وكالة حماية و تهيئة الشريط الساحلي

AGENCE DE PROTECTION ET D'AMENAGEMENT DU LITTORAL

- CONSULTATION –
AUDIT DE SECURITE INFORMATIQUE

Décembre 2017

SOMMAIRE

Cahier des Clauses Administratives Particulières---------- Page 3

Cahier des Clauses Techniques Particulières---------- Page 14

Méthodologie de Dépouillement---------- Page 28

Annexes---------- Page 30

Annexe A1 : Description Technique du système à auditer & Description Volumétrique des structures à auditer----------Page 31

Annexe A2: Organigramme global des entités à auditer----------Page 38

FORMULAIRES DES REPONSES---------- Page 41

Annexe 1 : Références du soumissionnaire ----------Page 41

Annexe 2 : Qualité des Moyens humains mis à la disposition de la mission ----------Page 37

Annexe 3 : Méthodologie de conduite du projet ----------Page 39

Annexe 4 : Planning prévisionnel de la mission ----------Page 42

Annexe 5 : Modèle type des CVs individuels ----------Page 44

Annexe 6 : Description des outils techniques utilisés----------Page 45

Annexe 7 : Déclaration sur l'honneur de confidentialité----------Page 46

Annexe 8 : Modèle de bordereau des prix----------Page 50

Annexe 9 : Description du système d'information de l'organisme----------Page 51

Cahier des Clauses Administratives Particulières

(Partie I)

ARTICLE 1 - OBJET DE LA CONSULTATION

L'APAL propose de lancer une consultation auprès des sociétés de service et d'ingénierie informatique, personnes morales certifiées par l'Agence Nationale de la sécurité Informatique conformément au décret 1249-2004 du mai 2004, 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 de charges.

ARTICLE 2 - DEFINITIONS ET INTERPRETATIONS

Maître d'Ouvrage	Désigne l'Agence de Protection et d'Aménagement du Littoral 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 consultation 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 ayant droit légaux du dit 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 du marché.
Audit sécurité	Signifie l'intervention de spécialistes, utilisant des techniques et des méthodes adéquates, pour évaluer la situation de la sécurité d'un système d'information et les risques potentiels.
Système d'information (SI)	Désigne l'ensemble des entités et moyens (structures, personnel, 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 de la Sécurité Informatique

ARTICLE 3 - CONDITIONS DE PARTICIPATION

Cette consultation s'adresse aux entreprises opérant dans le domaine d'audit et de la sécurité informatique, personne morales certifiées par **l'Agence Nationale de Sécurité Informatique (ANSI)** conformément au décret N° 2004-1249 du 25 mai 2004.

ARTICLE 4 - DUREE DE VALIDITE DES OFFRES

Les soumissionnaires resteront liés par leurs offres pendant un délai de soixante (60) jours à partir de la date limite de réception des offres.

Les soumissionnaires ne peuvent, pour aucun motif, revenir pendant cette période sur les prix et conditions de l'offre.

Le soumissionnaire doit se conformer sans formuler aucune réserve aux stipulations de toutes les clauses prévues dans le présent dossier de la consultation.

ARTICLE 5 - P R I X

Le Maître d'Ouvrage entend contracter des missions d'audit à prix Homme/jour forfaitaire (tous frais inclus) par catégorie d'intervenant, qui devra être pris comme base de prix pour déterminer le coût de l'offre. Il n'acceptera aucune augmentation de ces prix Homme/jour forfaitaires, quelle qu'en soit la raison.

Le prix de l'offre globale doit être obligatoirement présenté en chiffres et en lettres détaillés comme suit :

En hors TVA et en toutes taxes comprises (indiquer le taux de la TVA) pour la mission d'audit de la sécurité du système d'information.

Le tableau des prix doit être obligatoirement rempli par le soumissionnaire.

ARTICLE 6 – PRESENTATION DE L'OFFRE

Les offres doivent parvenir sous plis fermé par porteur ou par voie postale à l'APAL au plus tard la date mentionnée dans l'avis, le cachet du bureau d'ordre central fait foi.

Les soumissions doivent être placées dans une enveloppe constituée par :

A- Les pièces administratives :

1. Fiche de renseignements généraux.
2. Attestation d'affiliation à la Caisse Nationale de la Sécurité Sociale valable a la date d'ouverture, des auditeurs certifiés (membres de l'équipe intervenante).
3. Les copies conformes des certificats des auditeurs certifiés (membres de l'équipe intervenante).
4. Une copie conforme du certificat du soumissionnaire.

B-L'offre technique et financière

Ordre	Section
1	Le cahier des charges signé et paraphé page par page y compris les annexes, les notices techniques APAL.
2	Le tableau des prix.
3	Présentation des références du soumissionnaire (selon le modèle fourni dans l'annexe 1 des formulaires des réponses à remplir par le soumissionnaire).
4	Méthodologie(s) proposée(s) pour la conduite du volet audit organisationnel et physique de chaque composante du SI, incluant le détail du planning prévisionnel de la mission (équipe intervenante, charge H/J), et la spécification des outils logiciels d'accompagnement (traitement des enquêtes et calcul de risque) et des modèles de formulaires des réponses à remplir par le soumissionnaire, y afférents, remplis, avec soin et précision (annexe 2 et 3).
5	Méthode(s) proposée(s) pour la conduite du volet audit technique, incluant la spécification des outils et scripts à utiliser lors de ce volet de l'audit et le détail du planning prévisionnel d'exécution, accompagnée des modèles des formulaires des réponses à remplir par le soumissionnaire, y afférents, remplis, avec soin et précision (annexe 3). Descriptif des opérations de sensibilisation, accompagnée des références des intervenants et d'une description de la matière de sensibilisation (documents/maquettes, ...) qui sera utilisée (annexe 3). Le tableau récapitulatif, résumant la démarche d'audit proposée (annexe 3 de la liste des formulaires de réponses à remplir par le soumissionnaire)
6	Le planning prévisionnel de la mission, spécifiant clairement toutes les phases d'exécution, accompagné des modèles de l'annexe 4 des formulaires des réponses à remplir par le soumissionnaire y afférents, remplis, avec précision.
7	CVs et références de l'équipe d'audit proposée, conformément au modèle fourni en annexe 5 de la liste des formulaires à remplir par le soumissionnaire, accompagnés de toutes les pièces justificatives nécessaires.
8	Description des Outils techniques utilisés, conformément au modèle fourni en annexe 6 des formulaires des réponses à remplir par le soumissionnaire.
9	Les Déclarations sur l'honneur, de confidentialité, de la société et des auditeurs qui seront impliquées dans les réunions d'éclaircissement et de visite sur terrain, préliminaires à la soumission de l'offre (annexe 7 des formulaires des réponses à remplir par le soumissionnaire).

Le soumissionnaire doit mentionner sur l'enveloppe contenant son offre les indications suivantes :

AGENCE DE PROTECTION ET D'AMENAGEMENT DU LITTORAL
2 Rue Mohamed Rachid Ridha 1002 Belvédère – Tunis.
« NE PAS OUVRIR MISSION
AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION »

Toute offre non conforme à ces dispositions, ou adressée par fax ou parvenue après la date limite de réception des offres ne sera pas examinée quel que soit le motif et sera écartée.

ARTICLE 7 - MISSION DE RECONNAISSANCE

En vue de l'élaboration de leur offre les soumissionnaires pourraient entreprendre, à leurs frais des missions préalables de reconnaissance, auprès des structures à auditer. Ils devront présenter une demande écrite au Maître d'Ouvrage, qui notifiera ce fait à tous ceux qui décidera de la date de la visite, au moins vingt (20) jours ouvrables avant la date finale de remise des offres.

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 quinze (15) jours ouvrables avant la date de remise des offres, via une notification écrite à tous les concernés.

ARTICLE 8 - CRITERES D'EVALUATION DES OFFRES

L'évaluation technique et financière des offres reçues sera faite sur la base des critères détaillés à la méthodologie de dépouillement des offres.
L'offre conforme techniquement et ayant la meilleure note globale (NG) résultat de l'application de la méthodologie de dépouillement sera retenue.

ARTICLE 9 - DUREE DE REALISATION DES MISSIONS

La durée de réalisation de la mission objet de la présente consultation, **ne doit pas dépasser 40 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, auquel seront rajoutées les délais additionnels éventuels pris pour la correction (validation) des différents livrables exigés dans le présent cahier des charges, ainsi que ceux spécifiés dans l'offre.

ARTICLE 10 - ATTRIBUTION

L'offre ayant obtenu la meilleure note finale sera considérée l'offre la plus avantageuse. En cas d'égalité de note finale, celle ayant obtenu la meilleure note technique sera considérée l'offre la plus avantageuse parmi les offres conformes à l'objet de la commande et aux conditions du présent cahier des charges.

ARTICLE 11 – CAUTIONNEMENT DEFINITIF

Dans les vingt (20) jours qui suivent la notification de la commande par l'APAL, le titulaire de la commande doit fournir une caution définitive égale à trois pour cent (3%) de la valeur de la commande afin de garantir la bonne exécution de ses obligations et le recouvrement des sommes dont il serait reconnu débiteur au titre de la commande qui découlerait de la présente consultation.
Cette caution dont le texte figure en annexe 1 de la présente consultation doit être valable quatre (4) mois après la date de la réception définitive.
La libération de cette caution est conditionnée par le fait que le titulaire de la commande ait rempli à cette date toutes ses obligations au regard de l'APAL. et sans que la moindre réserve n'ait été formulée par cette dernière.

ARTICLE 12 - MODALITES DE PAIEMENT

Les paiements seront effectués comme suit:
- 80% du montant total de la commande seront payés par virement bancaire dans les quarante cinq (45 jours qui suivent la réception et la validation du rapport **final** d'audit des structures auditées.
- 20% du montant total de la commande seront payés par virement bancaire dans les quarante cinq (45) jours qui suivent la validation de l'ANSI.

ARTICLE 13 - PENALITES DE RETARD

En cas de retard, dans l'exécution de la mission d'audit sécurité, par rapport aux délais définitivement fixés, il sera appliqué de plein droit et sans mise en demeure préalable au fournisseur par jour de retard, une pénalité de un pour mille (1°/°°) de la valeur de la commande.
Cette pénalité est plafonnée à 5 % du montant de la commande augmenté le cas échéant du montant de ses avenants.
Les pénalités de retard commencent à courir à partir de l'échéance de l'entrée en vigueur de la commande.

ARTICLE 14 – RECEPTION

La réception des missions d'audit s'effectuera pour la totalité de la commande.
Le Maître d'Ouvrage appliquera deux phases de réception :

1- Première phase : La première phase consiste en l'approbation par le Maître d'Ouvrage du rapport préliminaire d'audit de la structure auditée.

Ce rapport d'audit devra couvrir au minimum les sections spécifiées dans les paragraphes a), b) et c) de l'article 4 du cahier des clauses techniques (livrables).

Le chef de Projet désigné parle Maître d'Ouvrage donnera son avis quant à la consistance et la pertinence du rapport, en regard :

- A la qualité de réalisation des objectifs assignés à la mission et fixés dans le Cahier des Clauses Techniques et, le cas échéant, tel que raffinées 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 issues.
- Le cas échéant, de la qualité des mesures d'accompagnement consignées.

Le Maître d'Ouvrage se chargera de communiquer cet avis au titulaire dans un délai ne dépassant pas quinze (15) jours ouvrables à partir de la date de réception du rapport.

Au cas où l'avis consigne des réserves, le titulaire devra lever ces réserves, dans une période ne dépassant pas quinze (15) jours ouvrables à partir de la date de leur notification, sauf accord contraire entre les deux parties, compte tenu du volume des corrections.

Le cas échéant et en cas de conflit insoluble sur les réserves formulées, et après avoir entamé toutes les procédures de rapprochement nécessaires, le Maître d'ouvrage et éventuellement le titulaire pourraient demander l'arbitrage de l'ANSI ou d'un expert auditeur certifié, pour décider de la suite à donner à ce conflit, avant d'intenter une procédure de résiliation et éventuellement pénale. En cas d'arbitrage, le titulaire pourrait être appelé à fournir les documents nécessaires pour l'arbitrage et en cas de besoin de refaire certains tests.

2- Deuxième phase : Cette phase consiste en la soumission du rapport final d'audit à l'approbation du Maître d'Ouvrage.

Ce rapport devra être remis par le soumissionnaire dans les délais impartis (en tenant compte de l'éventuel rallongement induit par la phase 1). Tout retard imputé au titulaire donnera lieu à l'application de la clause de pénalité du présent Cahier des Clauses Administratives.

Le chef de Projet du Maître d'Ouvrage 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) de recommandations issues des travaux d'audit et de leurs complétudes.

De la qualité des plans d'action et de l'esquisse du schéma directeur.

Le Maître d'Ouvrage se chargera de communiquer cet avis au titulaire dans un délai ne dépassant pas quinze (15) jours ouvrables à partir de la date de réception du rapport.

Au cas où l'avis consigne des réserves, le titulaire devra lever ces réserves, dans une période ne dépassant pas quinze (15) jours ouvrables à partir de la date de leur notification, sauf accord contraire entre les deux parties, compte tenu du volume des corrections.

En cas de conflit insoluble et après avoir entamé toutes les procédures de rapprochement nécessaire, le Maître d'ouvrage 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 (auditeur certifié) 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 15 - 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. Le Maître d'Ouvrage interdit aux soumissionnaires et au titulaire de délivrer via n'importe quel moyen de communication, toute information confidentielle relative au SI et spécialement toute information pouvant :

- Donner une indication sur l'architecture réseau, la configuration matérielle ou logicielle, les plates-formes, les serveurs, ... 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.

Durant et au terme de la mission, le titulaire s'engage à ne divulguer ou à déposer dans des lieux non sécurisés tout document, quelque soit sa forme (papier, magnétique, électronique ou autre), portant des informations concernant les structures auditées. Il veillera à la fin de la mission à détruire les documents de travail utilisés ou à assurer leur stockage dans un lieu ou sous un format hautement sécurisé. Le maître d'ouvrage se réserve le droit de vérifier le niveau de sécurité des endroits de stockage de documents relatifs à la mission et ce à tout moment, même postérieur à la mission.

ARTICLE 16 - PROPRIETE DES DOCUMENTS

Tous les rapports et documents produits en exécution de la présente consultation sont la propriété exclusive du Maître d'Ouvrage. Le titulaire ne peut les distribuer, les diffuser, ou les communiquer sous quelque forme que ce soit sans le consentement écrit du Maître d'Ouvrage.

ARTICLE 17 - APPROBATION DE L'AUDIT PAR L'ANSI

Le rapport final doit être remis à l'Agence Nationale de la Sécurité Informatique conformément aux dispositions du décret 1250-2004.Si le rapport d'audit était 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 18 - DUREE DU CONTRAT

La découlant de la présente consultation aura une durée d'une année à compter de sa date d'entrée en vigueur.

Il se renouvellera par tacite reconduction 2 fois au maximum, à moins d'un congé signifié au terme du contrat par l'une des deux parties par lettre recommandée avec un préavis d'au moins trois mois. il demeure entendu que toute reconduction du contrat est tributaire de la fourniture de l'attestation d'assurance et ce dans un délai d'un mois. A défaut de fourniture de la dite attestation, le contrat sera résilié.

Outre la résiliation pour fin de terme, le contrat découlant de la présente consultation peut être résilié en cas de non-observation par l'Entreprise de l'une de ses différentes obligations contractuelles.

ARTICLE 19- RESILIATION DE LA COMMANDE

La commande peut être résilié par décision du Maître d'Ouvrage aux torts du titulaire dans le cas où :

- Le cautionnement définitif n'a pas été déposé.
- Le titulaire déclare ne pas pouvoir exécuter ses engagements sans qu'il puisse invoquer un cas de force majeur, entre autres en modifiant la constitution des équipes proposées dans son offre, sans autorisation préalable du maître d'ouvrage.
- Le titulaire se permet de violer les dispositions de l'article « secret professionnel ».
- Le titulaire a perturbé de manière très grave la continuité du service du système audité (plus de huit (8) heure de travail de perturbation de fonctionnement), en ayant procédé à des tests connus pour être dangereux, sans préavis et autorisation préalable.
- Le titulaire se livre, à l'occasion de la commande, à des actes frauduleux portant sur la nature, ou la qualité de ses missions.
- Le titulaire commet de graves négligences dans la conduite des missions d'audit ou dans ses relations avec le Maître d'Ouvrage ou la structure à auditer.
- Le titulaire a fait soit par lui même soit par une autre personne interposée des promesses, des dons ou des présents en vue d'influencer les différentes procédures de conclusions de la commande et/ou les étapes de sa réalisation.

Le Maître d'Ouvrage se réserve le droit de faire exécuter la commande par un tiers aux frais et risques de la partie aux torts de laquelle la résiliation est prononcée.

La résiliation de la commande ne fera pas obstacle à la mise en œuvre des actions civiles ou pénales qui pourraient être intentées contre le titulaire en raison de ses fautes.

Le titulaire s'engage à ne plus procéder, dès réception de la décision de Maître d'Ouvrage, qu'à des opérations de liquidation de la commande.

ARTICLE 20 - ENTREE EN VIGUEUR

La commande qui découlerait de la présente consultation entrera en vigueur dès sa notification au fournisseur.

LE SOUMISSIONNAIRE
LU & APPROUVE
DATE, SIGNATURE & CACHET

ANNEXE 1

Modèle d'engagement d'une caution personnelle et solidaire

(À produire au lieu et place du cautionnement définitif)

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

1) Certifie - certifions que (3) ..... a été agréé par le Ministre des Finances en application de l'article 113 du décret 1039 du 13 mars 2014 portant réglementation des marchés publics, tel que modifié et complété par les textes subséquents, 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 .....le cautionnement fixe de cinq mille dinars (5000 dinars) prévu par l'article 113 du décret susvisé et que ce cautionnement n'a pas été restitué.

2) Déclare me - déclarons nous, porter caution personnelle et solidaire (4) ..... domicilié à (5) ..... Au titre du montant du cautionnement définitif auquel ce dernier est assujetti en qualité de titulaire du marché n° .....passé avec (6)..... en date du ..... enregistré à la recette des finances (7)..... relatif à (8) ..... Le montant du cautionnement définitif, s'élève à ..... % du montant du marché, ce qui correspond à .....dinars (en toutes lettres), et à .... dinars (en chiffres).

3) M'engage - nous nous engageons solidairement, à effectuer le versement du montant garanti susvisé et dont le titulaire du marché serait débiteur au titre du marché susvisé, et ce, à la première demande écrite de l'acheteur public sans que j'ai (nous ayons) la possibilité de différer le paiement ou soulever de contestation pour quelque motif que ce soit et sans une mise en demeure ou une quelconque démarche administrative ou judiciaire préalable.

4) En application des dispositions de l'article 108 du décret 1039 du 13 mars 2014 susvisé, la caution qui remplace le cautionnement définitif devient caduque à condition que le titulaire du marché se soit acquitté de toutes ses obligations, et ce à l'expiration du délai de quatre mois à compter de la date de la réception définitive

Si le titulaire du marché a été avisé par l'acheteur public avant l'expiration du délai susvisé, par lettre motivée et recommandée ou par tout autre moyen ayant date certaine, qu'il n'a pas honoré tous ses engagements, il est fait opposition à l'expiration de la caution. Dans ce cas la caution ne devient caduque que par main levée délivrée par l'acheteur public.

Fait à ....., le .....

(1) Nom(s) et prénom(s) du (des) signataire(s)
(2) Raison sociale et adresse de l'établissement garant
(3) Raison sociale de l'établissement garant
(4) Nom du titulaire du marché
(5) Adresse du titulaire du marché
(6) Acheteur public
(7) Indication des références d'enregistrement auprès de la recette des finances
(8) Objet du marché

ANNEXE 2

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE

Je soussigné M. ……., expert auditeur , certifié par l'Agence Nationale de la Sécurité Informatique et faisant partie du personnel permanent de notre société ……., déclare sur l'honneur maintenir une confidentialité totale sur toute information contenue dans le cahier des charges, objet de la consultation « **mission d'audit sécurité du système d'information de l'APAL**, acquis pour le compte de la société…….. …….. que je représente et organisée par l'APAL.

Mr …….,

CIN N° ……..

(Cachet de la société et signature)

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

(Partie II)

ARTICLE 1 - OBJET DE LA CONSULTATION

L'APAL se propose de lancer une consultation auprès des sociétés de services et d'ingénierie informatique pour effectuer une mission d'audit de la sécurité de son système d'informations conformément aux dispositions du décret N°2004-1250 du 25 mai 2004 et aux dispositions du présent cahier des charges. Cette mission doit être pilotée par, un chef de projet certifié par l'Agence Nationale de Sécurité Informatique (ANSI), conformément au décret n°004-1249 du 25 mai 2004. Elle est annuelle et renouvelable par tacite reconduction avec une durée maximale de trois (3) ans.

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

La mission d'audit devra ainsi concerner les aspects organisationnels, physiques et techniques relatifs à la sécurité du système d'information inclus dans le périmètre de cet audit.

« L'entreprise désirant participer à cette consultation est tenue de présenter une offre relative aux deux phases d'accompagnement pré et post-audit sans engagement de la part du commanditaire de l'audit de lui attribuer leur réalisation. »

ARTICLE 2: METHODOLOGIE(S) ADOPTEE (S)

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

La (ou les) méthodologie(s) adoptée(s) devra(ont) être adaptée(s), dans leur mise en œuvre, à la réalité, métier et taille des entités auditées et devra(ont) permettre d'aboutir à l'élaboration de bilans, de recommandations et de 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, urgence et faisabilité des actions à mener.

Ainsi, le soumissionnaire est appelé à indiquer, clairement dans son offre, la (ou les) méthodologie(s) d'audit qu'il envisage de mettre en œuvre, tout en fournissant des références sur son adéquation avec le référentiel ISO/CEI 27002. L'APAL tiendra compte dans son évaluation de la consistance de la (ou des) méthodologie(s) proposée(s), ou

parties de ces méthodologies et ce à chaque phase ainsi que de son adéquation à la réalité de l'entreprise et du temps imparti.

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

Le soumissionnaire doit spécifier dans la rubrique « Planning prévisionnel de la mission », au minimum, et pour chaque composant du système d'informations :

Le type de la méthodologie à mettre en œuvre pour le volet physique et organisationnel et les structures recensées utiles à interviewer, ainsi que les outils logiciels accompagnant la mise en oeuvre de cette méthodologie (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 leur objectif, ainsi que les outils utilisés,

La séquence des actions à mener (interviews, tests techniques, synthèse, rédaction de rapports,...) et une estimation de la charge homme/jour de chaque action, incluant un résumé des corrections de volumétrie proposées par rapport à l'estimation préliminaire proposée dans le cahier des charges,

La liste nominative des équipes qui interviendront pour chaque composant (site, structure) avec référence de l'expérience dans la mise en œuvre de la (des) méthodologie(s) et 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 l'APAL (avec insertion de ces écrits dans le rapport final). De plus, le personnel en charge de l'audit doit être du 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 doit 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.

Le soumissionnaire doit inclure dans son offre une présentation des CVs des intervenants (en prenant comme base, le modèle fourni en annexe 5 du présent cahier de charges).

ARTICLE 3 – CONDUITE ET DEROULEMENT DE LA MISSION

La mission d'audit, objet de la présente consultation, doit couvrir les aspects physiques, organisationnels et techniques, relatifs à la sécurité de l'ensemble des entités et moyens suivants : structures, personnel, outils logiciels, équipements de traitement, équipements réseaux, équipements de sécurité,... en relation avec les fonctions de traitement de l'information au niveau de l'APAL.

La description du système d'information de l'APAL est fournie en annexe A1 du présent cahier des charges.

Les sites décrits en annexe A2 du présent cahier des charges constituent un seuil minimum d'entités à auditer en se déplaçant physiquement sur les lieux.

La conduite de la mission et notamment les différentes réunions préparatoires de lancement ainsi que les séances de validation des rapports de chaque phase doivent être obligatoirement menées, du côté du titulaire de la commande, par le chef de projet certifié par l'Agence Nationale de Sécurité Informatique.

La mission objet de la présente consultation sera décomposée en cinq phases :

3.1 Phase 1 : Préparation de la mission

3.1.1 Accompagnement Pré-audit

Cette phase consiste à assister l'APAL à définir les besoins de sécurité de son système d'information par rapport aux objectifs de sécurité (Confidentialité, Intégrité, Disponibilité et Non Répudiation).

Cette définition des besoins permettra à l'auditeur de proposer les exigences minimales de sécurité pour ce système d'information et de choisir les contrôles de sécurité appropriés à appliquer.

Le processus de sélection de ces contrôles doit impliquer la direction et le personnel opérationnel au sein de l'organisme.

3.1.2 Actions de lancement de la mission

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

Des réunions préparatoires de la mission seront organisées au début de la mission, dont l'objet sera de finaliser, sur la base des besoins et documents préparés par le soumissionnaire retenu, les détails de mise en œuvre de la mission.

Elles concerneront, sans s'y limiter, la finalisation des détails suivants :

- Désignation des chefs de projets et des interlocuteurs, côté APAL et titulaire de la commande,
- Fourniture par l'APAL des détails complémentaires, relatifs au périmètre de l'audit (si le titulaire de la commande fait recours à l'échantillonnage, il est tenu d'en présenter les critères pour chaque type d'objet de l'audit),
- Validation du périmètre de l'audit,
- Fourniture par l'APAL des documents requis pour l'audit (Manuels d'exploitation, schémas d'architectures, ...),
- Fourniture du document de définition des besoins de sécurité. Si ce document n'existe pas, le maitre d'ouvrage tâchera à le préparer et le fournira au titulaire avant le démarrage de l'audit sur site,
- Détermination de la conformité des documents existants aux exigences de la norme ISO/IEC 27002, arrêt de la liste des documents manquants exigés par cette norme et examen des problèmes éventuels, relatifs à la mise à jour de la documentation,
- Examen des détails des listes des interviews à réaliser par le soumissionnaire et fourniture par l'APAL de la liste nominative des personnes à interviewer,
- Affinement des plannings d'exécution (planning des actions/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 devrait être élaboré sur la base d'études de terrain, octroi de locaux de travail au soumissionnaire retenu, ...).

Ainsi tous les détails de mise en œuvre doivent être examinés et validés. Ces réunions déboucheront, entre autre, sur la finalisation 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.

En cas de difficultés notoires rencontrées lors de cette phase, le titulaire devra faire recours au Maître d'Ouvrage par écrit, pour lui permettre d'intervenir efficacement et dans les délais.

3.1.3 Actions de sensibilisation pré-audit

Dans l'objectif de sensibiliser les responsables et acteurs du système d'informations de l'APAL, des actions de sensibilisation préliminaires seront assurées par le titulaire de la commande. Ces actions auront pour premier objectif une sensibilisation générale sur les dangers cybernétiques et les risques cachés encourus, incluant entre autres la présentation pratique d'attaques cybernétiques. Ces actions doivent aussi rechercher l'octroi de la transparence et collaboration des utilisateurs, en rappelant les objectifs de l'audit, l'urgence et 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 le maitre d'ouvrage et des fiches d'évaluation de ces sessions seront remplies par les participants. Des copies de ce PV et de ces fiches seront jointes au rapport d'audit.

A cet effet, le soumissionnaire doit inclure dans son offre, la réalisation de 3 sessions de sensibilisation pré-audit de 3 heures chacune.

Il doit inclure dans son offre, les références des animateurs de cette opération, ainsi qu'une description de la matière de sensibilisation (documents/maquettes, profils ciblés, ...) qui sera utilisée. Ces animateurs doivent avoir une bonne expérience dans l'animation de ce genre d'opération.

3.2 Phase 2 : Audit sur terrain

C'est la phase d'audit proprement dite. Pour les sites précisés en annexe A2, l'équipe intervenante du titulaire de la commande doit obligatoirement auditer ces entités en se déplaçant physiquement sur les lieux. Pour le reste des sites et entités de l'APAL, l'équipe intervenante du titulaire de la commande effectuera l'audit moyennant des outils et des

tests à distance et convoquera le personnel de ces sites, au siège de l'APAL, pour réaliser les interviews. Il est bien entendu que pour les sites non inclus dans l'annexe A2, l'équipe intervenante du titulaire de la commande pourrait éventuellement effectuer l'audit sur les lieux si elle le juge nécessaire.

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.

3.2.1 Volet audit organisationnel et physique

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. Ce volet doit couvrir les aspects de gestion et d'organisation de la sécurité, sur les plans organisationnels, humains et physiques.

Au cours de cette étape, le titulaire de la commande doit adopter 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 l'identification et classification des ressources relativement à leur criticité.

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

3.2.2 Volet audit technique

3.2.2.1 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 du système d'informations et particulièrement du réseau. Cette analyse doit 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'intrusions et tout autres tests permettant d'apprécier la robustesse de la sécurité du système d'informations et sa capacité à préserver les aspects de confidentialité, d'intégrité, de disponibilité et d'autorisation.

Au cours de cette étape, le titulaire de la commande doit, 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,
- Evaluer, la vulnérabilité et solidité des composantes matérielles et logicielles du système d'informations (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, d'authentification, de 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'attaques, relais de spam, exploitation du PABX pour le détournement "vol" des lignes de communication, ...).

Cette phase doit 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.

Pour les tests intrusifs, l'auditeur doit s'engager à les effectuer sans compromettre la disponibilité, l'intégrité ou la confidentialité des systèmes et des réseaux. Ainsi, les tests réalisés ne doivent pas perturber la continuité de service du système audité. Les tests critiques, pouvant provoquer des effets de bord, doivent être notifiés à l'APAL et doivent 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.

3.2.2.2 Outils utilisés

Lors des audits techniques, l'utilisation d'outils commerciaux doit 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, ...).

De plus, étant donné qu'aucun produit commercial ne saurait prétendre, à lui seul, à une complétude totale, les outils disponibles dans le domaine du logiciel libre (et généralement utilisés par les attaquants) doivent être savamment déployés pour assurer une complétude correcte de cette phase, en s'appuyant, quand cela est possible, sur des scripts riches de mise en œuvre savante et combinée de ces outils.

Les outils proposés doivent 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-formes systèmes (OS, ..) présentes 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, ...),
- Outils de scan d'existence de connexions dial-up dangereuses (war-dialing).

Et tout autre type d'outil, recensé nécessaire, relativement aux spécificités du SI audité (test d'infrastructure de PKI, ...).

Le soumissionnaire doit fournir la référence et une description concise (résumé de la liste des fonctionnalités offertes) des outils et scripts qu'il compte utiliser, en spécifiant l'objectif, lieu (phase de l'audit) et types de fonctionnalités de l'outil ou script qui seront mises en œuvre (conformément au modèle en annexe 6).

3.2.3 Appréciation des risques

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'appréciation des risques se déroulera en deux étapes :

3.2.3.1 Etape 1 : Analyse

Dans cette phase 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. Evaluer la probabilité réaliste d'une défaillance de sécurité au vu des mesures actuellement mises en œuvre.

3.2.3.2 Etape 2 : Evaluation

Dans 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.

3.3 Phase 3 : Synthèse des recommandations – Sensibilisation post-audit

3.3.1 Synthèses des recommandations

Le titulaire de la commande doit, à la fin de la phase d'audit sur terrain, réaliser :

- un rapport daté, signé par le responsable de l'audit et portant le cachet du titulaire, énumérant la liste des failles (classées par ordre de gravité et d'impact) ainsi qu'une évaluation de leurs risques,
- les recommandations portant sur les actions détaillées correctives à entreprendre à court terme,

- 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.,
- un rapport de synthèse, destiné à la direction générale, qui inclura d'une manière claire (destiné aux décideurs) les importants résultats de l'estimation des risques, un résumé 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 schéma directeur proposé.

Les recommandations portant sur les actions détaillées correctives à entreprendre à court terme doivent 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 :

a) Les premières actions et mesures à entreprendre en vue d'assurer la sécurisation de l'ensemble du système d'informations 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 oeuvre, 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,

b) Une estimation des formations requises et des ressources humaines et financières supplémentaires nécessitées.

3.3.2 Actions de sensibilisations post-audit

Le titulaire de la commande doit, au cours de cette phase, réaliser des sessions de sensibilisation post-audit destinées aux responsables et aux acteurs du système d'informations de l'APAL.

Ces sessions auront pour objectif :

- Une sensibilisation aux failles décelées et aux risques cachés encourus,
- L'octroi de la collaboration des utilisateurs, pour ce qui concerne la mise en œuvre de la politique de sécurité proposée en spécifiant l'objectif de cette politique et les bienfaits attendus.

A la fin de cette opération un PV sera dressé et signé conjointement par le titulaire et le maitre d'ouvrage et des fiches d'évaluation de ces sessions seront remplies par les participants. Des copies de ce PV et de ces fiches seront jointes au rapport d'audit.

A cet effet, le soumissionnaire doit inclure dans son offre, la réalisation de 5 sessions de sensibilisation post-audit de 3 heures chacune.

Il doit inclure dans son offre, la référence des animateurs de cette opération, ainsi qu'une description de la matière de sensibilisation (documents/maquettes, profils ciblés, ...) qui sera utilisée. Ces animateurs doivent avoir une bonne expérience dans l'animation de ce genre d'opération.

3.4 Phase 4 : Evaluation de l'audit par l'ANSI

Le rapport final de l'audit doit être remis à l'Agence Nationale de la Sécurité Informatique pour validation et ce, conformément aux dispositions du décret 1250-2004 du 25 mai 2004.

Dans le cas où le rapport d'audit serait rejeté par l'Agence Nationale de Sécurité Informatique (ANSI) pour manquement grave aux prescriptions du décret 1250-2004, le titulaire de la commande est tenu de procéder à ses frais, à la correction des manquements signalés par l'ANSI et de remettre à l'APAL le nouveau rapport final de l'audit dans un délai ne dépassant pas un mois à compter du lendemain de la date de réception par le titulaire de la commande de la notification du rejet communiquée par l'APAL.

3.5 Phase 5 : Accompagnement Post-audit

Cette phase consiste à assister le Maître d'Ouvrage dans la mise en œuvre de toutes les recommandations émises dans le rapport d'audit, à savoir : la rédaction des documents de politique de sécurité, politique de sauvegarde, charte d'utilisation du système d'information, rédaction de divers cahier des charges pour les missions d'accompagnement,

ARTICLE4 – LIVRABLES

Pour les réceptions des phases de la mission d'audit objet du présent cahier des charges, le soumissionnaire retenu doit livrer à l'APAL les documents suivants :

1. Un rapport des actions de lancement de la mission couvrant les aspects précisés à l'article 3 – alinéa 3.1.2 du Cahier des Clauses Techniques Particulières (CCTP).
2. Un rapport d'audit qui doit couvrir, au minimum, les aspects mentionnés dans le décret N° 2004-1250 du 25 mai 2004 et les aspects exigés par les dispositions du présent cahier des charges et doit inclure au minimum les chapitres ou rapports suivants :

a) Une section relative à l'audit organisationnel et physique, cette section inclut :

- Une évaluation du niveau de la sécurité organisationnelle et physique de la sécurité du système d'information de l'APAL,
- Une analyse des risques encourus,

Une 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, cette section est composée en :

- Un audit des vulnérabilités existantes en précisant leur impact sur la pérennité des systèmes d'information et de communication de la structure ;
- Une analyse des risques encourus,
- Une liste des recommandations techniques à appliquer dans l'immédiat pour la correction des failles graves décelées.

Il est à noter que tous les travaux de test et d'analyse effectués doivent être consignés dans une annexe, en les ordonnant selon leur sévérité, en incluant au niveau du rapport un relevé des plus importantes failles et des moyens de les combler dans l'immédiat.

c) Une section relative au plan d'action et stratégie de sécurité à appliquer sur le court terme (jusqu'au prochain audit), comprenant des recommandations précises quant aux mesures à prendre dans le court terme, afin de pallier aux failles et insuffisances décelées, incluant 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.

1. Un rapport présentant un Plan Directeur sur trois années, permettant de mettre en œuvre une stratégie de sécurité cohérente et ciblée. Ce rapport sera mis en à jour lors des audits de la seconde et de la troisième année en tenant compte du taux de réalisation des mesures qui ont été adoptées depuis le dernier audit réalisé et des insuffisances enregistrées dans l'application des recommandations, ainsi que de l'audit de l'année en cours

2. Un rapport de synthèse, destiné à la direction générale, qui inclura d'une manière claire (destiné décideurs) les importants résultats de l'estimation des risques, un résumé 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 schéma directeur proposé.

Méthodologie de Dépouillement

(Partie III)

ARTICLE 1 – CRITERES DE CONFORMITE 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 nombre d'intervenants est de 2 personnes au minimum, sans compter le chef de projet,
3. Le chef du projet est un auditeur certifié par l'Agence Nationale de la Sécurité Informatique, conformément au décret susmentionné, en cours de validité,
4. L'expérience du chef de projet est supérieure ou égale à 7 ans,
5. Le chef de projet doit avoir piloté au moins 5 missions d'audit de sécurité des systèmes d'information pour le compte d'organismes de taille similaire,
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 pour le compte d'organismes de taille similaire,
8. Présentation de la méthodologie de conduite du projet conformément aux exigences citées en annexe 3.

ARTICLE 2 – CRITERES D'EVALUATION

S'agissant d'un marché d'études à caractère simple, 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 : La commission vérifiera les documents des offres et en particulier les montants et calculs relatifs aux prix. elle rectifiera éventuellement, le montant des offres sans que le Soumissionnaire puisse faire quelques objections que ce soit à ce sujet.
- La vérification de l'offre sera faite de la façon suivante :
- - Les offres seront vérifiées pour en rectifier les erreurs de calcul éventuelles, avant le classement financier. Les erreurs seront corrigées de la façon suivante :
- Lorsqu'il existe une différence entre le montant en chiffres et le montant en lettres, le montant en lettres fera foi ;
- - Les offres financières (toutes taxes comprises) ainsi présentées seront classées par ordre croissant et il sera procédé en premier lieu à la vérification de la satisfaction des qualifications techniques du soumissionnaire consulté le moins disant et à la détermination de ses aptitudes à exécuter le marché de façon satisfaisante conformément aux critères minimums exigés.

ANNEXES

ANNEXE A1

Description technique des systèmes à auditer

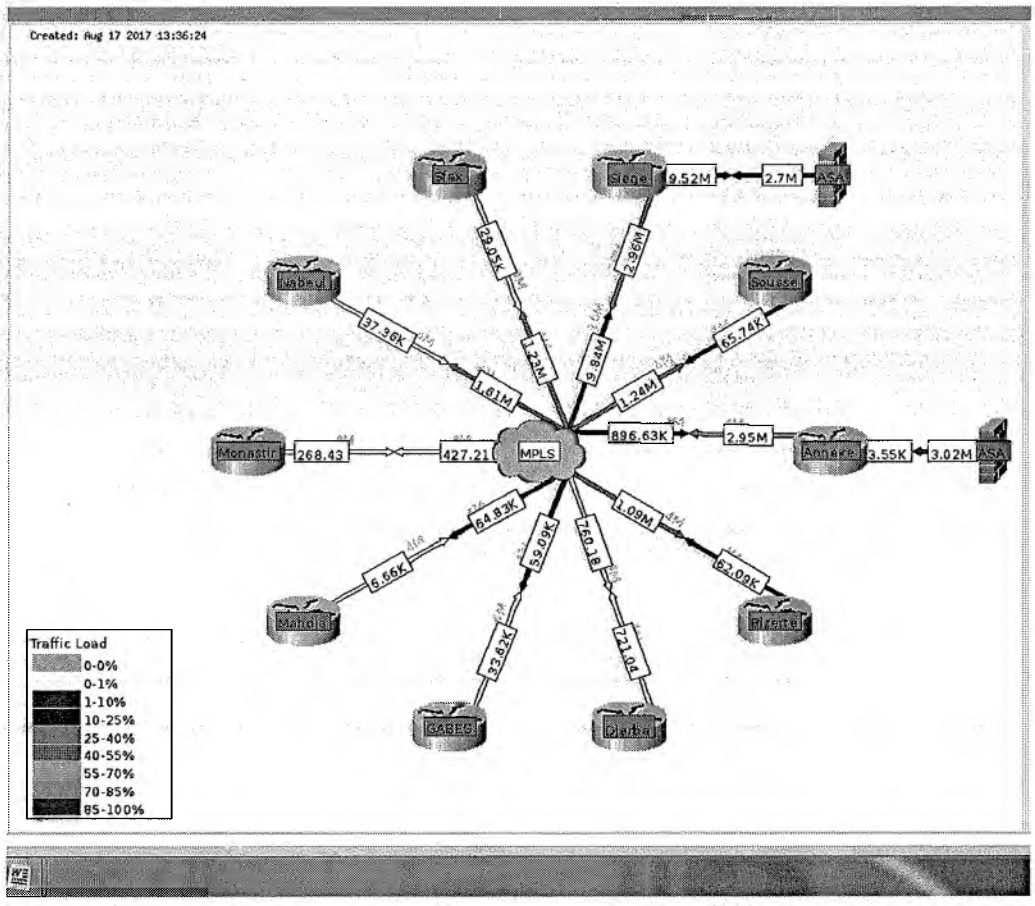
Description Volumétrique des structures à auditer	
	Volumétrie du Système d'Information
Sites à visiter et leur lieu	10
Nombre de responsables à interviewer	50
Centres de calcul à auditer	
Autres infrastructures spécifiques à auditer physiquement et/ou organisationnellement	La vidéo surveillance Trois sites hébergé en interne
Autre détails particuliers sur le niveau d'inspection physique ou/et organisationnel désiré	
PC	
Nb Total de PCs	
Type d'OS :	WIN XP, WIN 7
- Nombre moyen de PC sous Windows	160
- Nombre moyen de PC sous Mac OS	0
- Nombre moyen de PC sous Linux	0
Autres OS.	---
Serveurs	
Nombre Total de Serveurs	10
- Type d'OS	WIN Server 2003/2008/2012
- Nombre d'utilisateurs supportés	200
Applications	
Nombre d'applications (objet de l'audit de sécurité)	20
- Nombre d'utilisateurs	130
- Environnement des applications	SQL/ARCGIS
Réseau	
- Nombre de sites distants interconnectés	10
- Nombre de sous-réseaux (internes et externes)	10
- Connexions externes :	IPMPLS inter site
. Nombre de connexions permanentes, leur type (LS, FR,…) et leurs utilisations (Internet, inter-sites, avec des sites externes)	8 : SDSL 2 :FO 1 ADSL
. Nombre de Connexions Dial-Up et leurs utilisations (Internet, inter-sites, avec des sites externes)	2
. Nombre de routeurs et types de connexions supportées	9 :SDSL 2 : FO
Nombre de switchs et niveau (2,3,…)	3
Outils d'administration réseau et leurs types	0
Outils de Sécurité	
Firewalls	1 : ASA 5520 1 : ASA 5505
Nombre de systèmes de Firewalling, leurs types et Nombre de DMZs supportées	2
Type de connexions VPN activées au niveau des firewalls.	IPMPLS

Serveurs anti-virus	
Nombre de serveurs anti-virus et nombre de licences	1 serveur 120 licences
Nombre de passerelles anti-virales et leur usage (e-mail, web, FTP,…	1
Outils d'authentification	
Nombre de serveurs d'authentification réseau internes et nombre moyen d'utilisateurs supportés	1/ 80 Users
Nombre de serveurs d'authentification réseau pour les accès distants et nombre moyen d'utilisateurs supportés	0
Outils de détection d'intrusion	
Nombre de NIDS (IDS réseau)	0
Nombre de sondes HIDS (IDS hôte)	0
Nombre de Firewalls PC ou Distribués	0
Outils de sauvegarde automatique et leurs types	2 Robots HP LTO4
Outils intégrés d'administration de la sécurité et leurs types	0

Parc Informatique

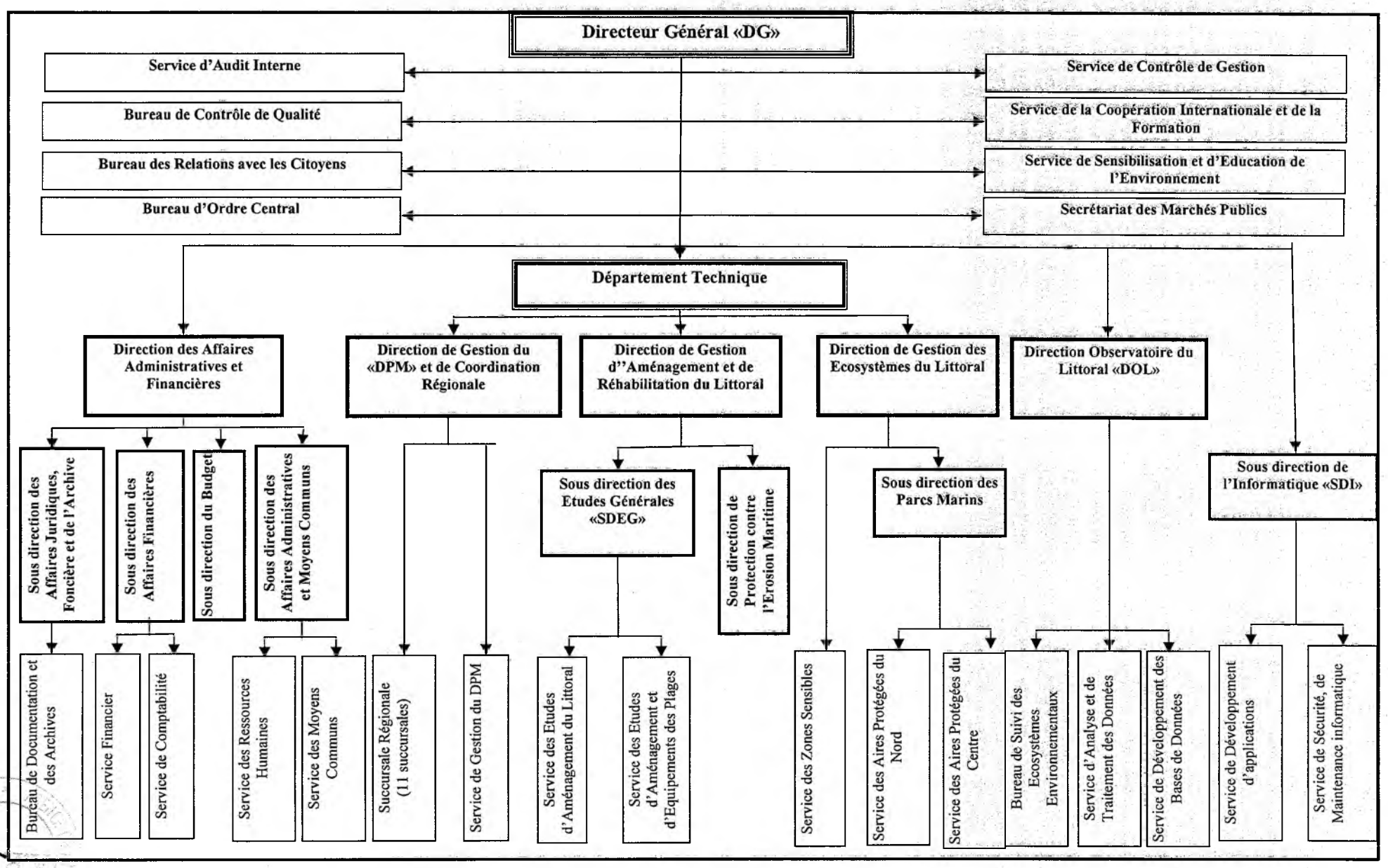
DESIGNATION	NOMBRE
BAIE DE DISQUE	**1**
COMMUTATEUR	**2**
CONSOLE	**2**
DIGITALISEUR	**2**
DISQUE DUR EXTERNE	**5**
FIREWALL	**2**
GPS	**4**
IMPRIMANTE	**80**
IMPRIMANTE RESEAU	**8**
ONDULEUR	**48**
ONDULEUR UPS	**2**
PC	**120**
PC PORTABLE	**40**
ROBOT DE SAUVEGARDE	**2**
SCANNER	**30**
SERVEUR	**10**
SWITCH	**12**
TABLETTE	**3**
TRACEUR	**2**

Architecture synoptique des sites à auditer



ANNEXE A2

Organigramme global des entités à auditer



Liste des structures à auditer, via un audit sur terrain

	Structure	Lieu d'implantation (gouvernorat)
1.	Siège APAL	Tunis, le belvédère
2.	ANNEXE APAL	Tunis, le belvédère
3.	U.R. Bizerte, Béja et Jendouba	Bizerte
4.	U.R. Nabeul	Korba
5.	U.R. Sousse	Sousse
6.	U.R. Monastir	Monastir
7.	U.R. Mahdia	Mahdia
8.	U.R. Sfax	Sfax
9.	U.R. Gabes	Gabes
10.	U.R. Medenine	Djerba

FORMULAIRES DES REPONSES

(A remplir et à insérer obligatoirement dans l'enveloppe de l'offre technique)

Réponse du Soumissionnaire :

La réponse est courte : doit figurer dans la colonne "Réponse du Soumissionnaire"
ou

La réponse nécessite le développement d'un chapitre : il faut préciser un indicateur de renvoi à ce chapitre tout en précisant, en référence, la question à laquelle se rapporte le chapitre détaillé.

ANNEXE 1

Références du soumissionnaire

Ordre	Sous-critère	Valeur minimale exigée	Réponse [1]
1	Spécialisation de l'entreprise dans l'activité d'audit sécurité	3 ans	
2	Nombre de missions dans l'activité de la sécurité Informatique (Intégration, Conseil, formation, ….)	05 missions	
3	Nombre des missions d'audit sécurité, conformes au décret N° 20041250, de plus de 20 Jours, effectuées durant les deux dernières années.	10 missions	
4	Effectif global du personnel Ingénieur (ou équivalent), affecté aux missions de sécurité informatique et d'audit	3 ingénieurs ou équivalent	
5	Effectif global d'analystes (ou équivalent) affectés aux missions de sécurité informatique et d'audit		
6	Effectif global des techniciens, affectés aux missions de sécurité informatique et d'audit		
7	Effectif technique global de l'entreprise	3	

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

ANNEXE 2

Qualité des Moyens humains mis à la disposition de la mission

Tableau 2.1

Compétence du chef du projet

Ordre	Sous-critère	Valeur minimale exigée	Réponse [1]
1	Expérience générale du chef du projet (en nombre d'années)	10 années	
2	Expérience en matière de sécurité informatique	5 années	
3	Nombre de Missions d'audit de plus de 20 jours et conformes au décret N° 2004-1250 conduites sous sa gestion directe en Tunisie ou à l'étranger, durant les deux dernières années.	10 missions	
4	Certifications et formations : ◈ Certifications obtenues en audit sécurité ◈ Certifications obtenues dans d'autres domaines de la sécurité informatique, en relation avec la mission ◈ Certifications obtenues dans des domaines en relation avec la mission (Plates-formes, Equipements réseau, méthodologies…) ◈ Formations, non certifiantes, suivies en audit sécurité ◈ Formations, non certifiantes, suivies dans d'autres domaines de la sécurité informatique, en relation avec la mission ◈ Formations, non certifiantes, suivies dans des domaines en relation avec la mission (Plates-formes, Equipements réseau, méthodologies…)		
5	Diplôme universitaire	Maîtrise en informatique ou télécom ou équivalent	
6	Expérience du chef du projet en tant que membre non chef de projet dans des opérations d'audit (en nombre de missions)		

Tableau 2.2

Qualité du personnel affecté à la mission

Tableau 2.2 : Qualité de l'équipe d'audit affectée à la mission

Ordre	Sous-critère	Valeur minimale exigée	Réponse [1]
1	Nombre des Ingénieurs (ou équivalent) affectés à la mission (Y compris le chef de projet)	3 ingénieurs ou équivalent	
2	Compétence des membres de l'équipe proposée	Voir tableau 2.2.1	

3	Nombre des membres certifiés par l'ANSI (autres que le chef du projet)	2 membres	
4	Un membre certifié ISO 27005	Une certification ISO 27005	
5	Un membre certifié CISCO ou équivalent	Une certification CCNA	
6	Un membre certifié Windows	Une certification MCP	

Tableau 2.2.1 : Compétence des membres de l'équipe proposée

Pour chaque intervenant employé à temps plein par le soumissionnaire

Ordre	Sous-critère	Valeur minimale exigée	Réponse
1	Expérience générale à partir de la date d'obtention du diplôme	5 années	
2	Expérience en matière de sécurité informatique	3 années	
3	Nombre de Missions d'audit conformes au décret 2004-1250 conduites durant les deux dernières années.	3 missions	
4	Diplôme universitaire	Ingénieur informatique ou équivalent	
5	Certifications et formations obtenues : ◈ Certifications obtenues en audit sécurité ◈ Certifications obtenues dans d'autres domaines de la sécurité informatique, en relation avec la mission ◈ Certifications obtenues dans des domaines en relation avec la mission (Plates-formes, Equipements réseau, méthodologies…) ◈ Formations, non certifiantes, suivies en audit sécurité ◈ Formations, non certifiantes, suivies dans d'autres domaines de la sécurité informatique, en relation avec la mission ◈ Formations, non certifiantes, suivies dans des domaines en relation avec la mission (Plates-formes, Equipements réseau, méthodologies…)		

Fait à : ……., le : ……

LE SOUMISSIONNAIRE
Nom, Prénom et qualité du signataire
Signature et Cachet

ANNEXE 3

Méthodologie de conduite du projet

1) METHODOLOGIE SUIVIE POUR L'AUDIT ORGANISATIONNEL & PHISYQUE ::

1. Décrire la (les) méthodologie(s) proposée(s) et indiquer les raisons de leur choix, ainsi que les références de leur adéquation avec la norme ISO/CEI 27002,
   ……
   ……
2. Structure du questionnaire à effectuer auprès des interviewés de l'audité, et les références d'adéquation des contrôles à vérifier à travers ce questionnaire avec la norme ISO 27002,
   ……
   ……
3. Fournir un échantillon du questionnaire à effectuer (électroniques le cas échéant),
   ……
   ……
4. Décrire les inspections à réaliser : types, description et résultats attendus,
   ……
   ……
5. Préciser les outils d'accompagnements utilisés pour le traitement des interviews, avec la liste des fonctionnalités et la documentation de chaque outil,
   ……
   ……
6. Décrire la méthodologie de calcul de risques et ses références,
   ……
   ……
7. Spécifier l'expérience de l'équipe dans la mise en œuvre de cette méthodologie (Formations, pratique de la méthodologie),
   ……
   ……

Fait à ……., le ……

LE SOUMISSIONNAIRE

Nom, Prénom et qualité du signataire

Signature et Cachet

2) METHODOLOGIE SUIVIE POUR L'AUDIT TECHNIQUE :

1. Décrire la méthodologie proposée, relativement à la nature de l'infrastructure.
   (Décrire l'approche méthodologique d'audit technique que le soumissionnaire entend appliquer)

   ……
   ……

   Spécifier les types de tests à effectuer et leurs objectifs (Audit de l'architecture, audit de la configuration de chaque type de composantes du périmètre de l'audit, audit intrusif) et en fournir une description,

   ……
   ……

   Spécifier les types d'inspections à réaliser (inspection topologique physique, autre)

   ……
   ……

2. Spécifier les types d'outils et scripts utilisés (fournir leurs références d'origine et une description et les résumer dans l'annexe 6)

   ……
   ……

   Spécifier la méthodologie d'analyse et de report des failles, selon leur gravité

   ……
   ……

   Expérience de l'équipe dans la mise en œuvre de cette méthodologie (pratique de la méthodologie, Formations sur les outils,..)

   ……
   ……

Fait à …….... le ……

LE SOUMISSIONNAIRE

Nom, Prénom et qualité du signataire

Signature et Cachet

3) DESCRIPTIF DES OPERATIONS DE SENSIBILISATION :

Description des opérations de sensibilisation :

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

Fait à ………..., le ……………

LE SOUMISSIONNAIRE

Nom, Prénom et qualité du signataire

Signature et Cachet

ANNEXE 4

Planning prévisionnel de la mission

Fournir pour chaque volet (organisationnel, technique et sensibilisation) les plannings détaillés d'exécution prévus pour chaque phase de la mission ainsi qu'un tableau récapitulatif des plannings d'exécution :

A/ Plannings détaillés d'exécution de la mission :

Phase 1 : Actions préparatoires de la mission

Actions	Intervenants	Logistique utilisée (outils, …)	Livrables	Durée en Hommes/Jour pour chaque intervenant		Durée (du … au …)
				Sur site	Totale	

Phase 2 : Audit sur terrain

Actions	Intervenants	Logistique utilisée (outils, …)	Livrables	Durée en Hommes/Jour pour chaque intervenant		Durée (du … au …)
				Sur site	Totale	

Phase 3 : Synthèse des recommandations – sensibilisation post-audit

Actions	Intervenants	Logistique utilisée (outils, …)	Livrables	Durée en Hommes/Jour pour chaque intervenant		Durée (du … au …)
				Sur site	Totale	

B/ Tableau récapitulatif des Plannings détaillés d'exécution de la mission :

Actions	Intervenants	Logistique utilisée (outils, …)	Livrables	Durée en Hommes/Jour pour chaque intervenant		Durée (du … au …)
				Sur site	Totale	

Fait à ……., le ……

LE SOUMISSIONNAIRE

Nom, Prénom et qualité du signataire

Signature et Cachet

ANNEXE 5
MODELE TYPE DES CVS INDIVIDUELS

Qualité dans le Projet :
- Chef de Projet
- Chef d'équipe
- Auditeur
- Consultant

Nom, Prénom, Age.....
Diplômes (universitaires) Obtenus : Type/Institution/année/Mention (fournir des copies)
Expérience professionnelle générale (décrire le cursus professionnel détaillé)
Expérience en matière de sécurité informatique
- Activités/projets réalisés en matière de sécurité informatique) :
  - développement,
  - conseil,
  - intégration,
  - Formation
  - Autres :
- Normes et Méthodologies d'audit maîtrisées :
- Outils d'audit technique maîtrisés
- Autres :

Expérience en matière d'audit
- Missions d'audit réalisées (exclusivement celles conformes à l'objet du décret 1250.) : références de la mission, durée, qualité (Chef de projet, chef d'équipe, auditeur, consultant) (avec fourniture de justificatifs).
- Certifications obtenues
  - Certifications obtenues en audit sécurité
  - Certifications obtenues dans d'autres domaines de la sécurité informatique, en relation avec la mission
  - Certifications éventuelles obtenues, en relation avec l'objet de la mission (avec fourniture de copies des certifications et des références de celle-ci) :

- Formations suivies

  - Formations, non certifiantes, suivies en audit sécurité
  - Formations, non certifiantes, suivies dans d'autres domaines de la sécurité informatique, en relation avec la mission
  - Formations, non certifiantes, suivies dans des domaines en relation avec la mission (Plates-formes, Equipements réseau, méthodologies…)

Qualification au sein de l'entreprise
- Contractuel/SIVP/ et Date de début d'activité au sein de la société
- Temps imparti à l'activité d'audit (Temps plein, Mi-temps, Autre)
- Autres activités pratiquées actuellement :
  - Développement
  - Intégration
  - Formation
  - Conseil
  - Autre :

Autres (références générales)

Fait à ....., le .....LE SOUMISSIONNAIRE

Nom, Prénom et qualité du signataire

Signature légalisée et Cachet

ANNEXE 6

DESCRIPTION DES OUTILS TECHNIQUES UTILISES

Description des outils utilisés dans l'audit technique pour les différentes catégories :

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-formes 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,….

Outils de scan de connexions dial-up.

Autres (autre type d'outil, recensé nécessaire, relativement aux spécificités du SI audité (test de l'infrastructure de PKI, ….).

Pour chaque catégorie, remplir le tableau suivant :

Outils	atégorie	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, ..)

Fait à ……., le ……

LE SOUMISSIONNAIRE

Nom, Prénom et qualité du signataire

Signature et Cachet

ANNEXE 7

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE

(Soumissionnaire)

Je soussigné Mr....., Responsable de la société ..... déclare désigner M. ..... Expert auditeur, certifié par l'Agence Nationale de la Sécurité Informatique et faisant partie du personnel permanent de notre société, pour nous représenter dans la réunion d'éclaircissement sur le contenu du cahier des charges, et préparatoire à la soumission de notre offre pour le marché ..... de l'Agence de Protection et d'Aménagement du Littoral : APAL.

Le Soumissionnaire

(Cachet et signature)

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 du personnel permanent de notre société, pour nous représenter dans la visite sur terrain, préparatoire à la soumission de notre offre pour le marché ..... de l'Agence de Protection et d'Aménagement du Littoral : APAL.

Le Soumissionnaire

(Cachet de la société et signature)

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE

(Délégué)

Je soussigné M. ……., expert auditeur , certifié par l'Agence Nationale de la Sécurité Informatique et faisant partie du personnel permanent de notre 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, l'Agence de Protection et d'Aménagement du Littoral : APAL.

Mr ……,

CIN N° ……..

(Cachet de la société et signature)

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 , l'Agence de Protection et d'Aménagement du Littoral : APAL.

Mr ……,

CIN N° ……..

(Cachet de la société et signature)

ANNEXE 8

MODELE DE BORDEREAU DES PRIX

(A remplir et à insérer obligatoirement dans l'enveloppe de l'offre financière)

Soumissionnaire : .....

Désignation	Prix HT		TVA	Prix TTC	
	En Chiffres	En Lettres		En Chiffres	En Lettres
Mission d'audit de sécurité du système d'informations de L'APAL					

Fait à : ....., le : .....

LE SOUMISSIONNAIRE

Nom, Prénom et qualité du signataire

Signature et Cachet

ANNEXE 9 : DESCRIPTION DU SYSTEME D'INFORMATION DE L'ORGANISME (à remplir par l'auditeur)

Pour chaque site:

Applications					
Nom (1)	Environnement de développement	Développée par /Année	Nombre d'utilisateurs	Mentionnée dans la description volumétrique (Annexe A1) (Oui/Non)	Incluse au périmètre d'audit (5)
…					

Serveurs				
Nom (1)	Système d'exploitation	Fonctionnalités (2)	Mentionné dans la description volumétrique (Annexe A1) (Oui/Non)	Inclus au périmètre d'audit (5)
…				

Infrastructure Réseau et sécurité					
Nature (3)	Marque	Nombre	Observations (4)	Mentionné dans la description volumétrique (Annexe A1) (Oui/Non)	Inclus au périmètre d'audit (5)
…					

Postes de travail			
Système d'exploitation	Nombre	Mentionné dans la description volumétrique (Annexe A1) (Oui/Non)	Inclus au périmètre d'audit (5)
…			

(1) : Veuillez respecter la même nomenclature utilisée au niveau du rapport d'audit.
(2) : Fonctionnalités : Base de données (MS SQL Server, Oracle, …), messagerie, application métier, Contrôleur de domaine, Proxy, Antivirus, etc.
Veuillez indiquer le(s) nom de (la) solutions métier au niveau de chaque serveur
(3): Nature: Switch, Routeur, Firewall, IDS/IPS, etc
(4) Observations : des informations complémentaires sur l'équipement par exemple niveau du switch
(5) : Oui/Non. Présenter les raisons de l'exclusion le cas échéant.

FICHE DES ELEMENTS DE CONTACT AVEC LE SOUMISSIONNAIRE

(A remplir et à insérer obligatoirement dans l'enveloppe de l'offre technique)

Soumissionnaire : …… ……
Adresse de courrier : ……..… …… …… Ville : …… Code Postal : ……...
Téléphone(s) N° : …… …… …… ……
Fax(s) N° : ……..…….. ……..
Adresse E-mail : …… ……

Fait à ……..…., le ……

LE SOUMISSIONNAIRE

Nom, Prénom et qualité du signataire

Signature et Cachet