République Tunisienne

Ministère de l'économie et de la planification

Office de Développement du Sud

« O.D.S »

___

Cahier des Charges

Pour

L'Audit de la sécurité du Système d'Information

de l'Office de Développement du Sud

____

Octobre 2024

Table des matières

Chapitre I - CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIERES

Article 1 : Objet de la consultation

L'Office de Développement du Sud 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 : Définition et interprétations

Maître d'Ouvrage	désigne l'Office de Développement du Sud (O.D.S) englobe les structures ou personnes dûment mandatées pour la supervision de cette mission.
Soumissionnaire	désigne toute entreprise 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 ayants droit légaux dudit prestataire.
Mission	signifie toute action d'audit, de test, de vérification y compris la rédaction des rapports, les déplacements, la collecte de données, l'analyse des tests, et toute autre action assurée par le titulaire pour le compte du Maître d'Ouvrage dans le cadre de la bonne exécution 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	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 Nationale de la Sécurité Informatique.

Article 3 : Condition de participation

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

Article 4 : Présentation de l'offre

Les offres doivent parvenir par voie postale sous pli fermé ou déposées directement au Bureau d'Ordre Central de l'Office de Développement du Sud (O.D.S), Immeuble Ettanmia – 4119 Médenine, au plus tard le **31…../10…./……2024**…., date limite de réception des offres (le cachet du bureau d'ordre central faisant foi).

Les offres qui parviennent après les délais sus-indiqués ne seront pas retenues.

Elles doivent être présentées, sous une enveloppe scellée contenant deux enveloppes une enveloppe A contenant l'offre technique et une enveloppe B contenant l'offre financière.

L'enveloppe extérieure doit être libellée au nom du **Directeur Général de l'Office de Développement du Sud et porter la mention :**
« A NE PAS OUVRIR – Consultation
AUDIT DE LA SECURITE DU SYSTEME D'INFORMATION ET DE COMMUNICATION
de l'Office de Développement du Sud »

En plus des enveloppes A et B l'enveloppe extérieure doit contenir les pièces suivantes :

- ✓ une copie conforme du certificat du soumissionnaire en cours de validité,
- ✓ les copies conformes des certificats des auditeurs membre de l'équipe intervenante en cours de validité,
- ✓ la déclaration trimestrielle des salariés et des salaires de la CNSS du dernier trimestre avant la date limite de remise des offres, des trois (3) auditeurs certifiés par l'ANSI et employés à temps plein par le soumissionnaire,
- ✓ les Déclarations sur l'honneur de confidentialité du soumissionnaire et des auditeurs qui seront impliqués, éventuellement, dans les réunions d'éclaircissement et de visite sur terrain, préliminaires à la soumission de l'offre (annexe 7).

L'Enveloppe A : doit porter la mention **« Offre technique »** et doit comporter les pièces suivantes :

- ✓ le cahier des charges et ses annexes avec paraphe et cachet humide au bas de chaque page. La signature de la dernière page doit être précédée de la date et de la mention manuscrite « Lu et approuvé »,
- ✓ un aperçu succinct sur l'activité générale du soumissionnaire, son organisation et son expérience dans le domaine,
- ✓ présentation des références du soumissionnaire (selon le modèle fourni dans l'Annexe 1),
- ✓ présentation de l'équipe intervenante (selon le modèle fourni dans l'Annexe 2),
- ✓ méthodologie(s) proposée(s) pour la conduite du volet audit organisationnel et physique, incluant la spécification des outils logiciels d'accompagnement (traitement des enquêtes et calcul de risque) selon le modèle de l'Annexe 3 y afférent, remplis avec soin et précision,
- ✓ méthodologie proposée pour la conduite du volet audit technique, incluant la spécification des outils et scripts à utiliser selon le modèle de l'Annexe 3 y afférents, remplis avec soin et précision,
- ✓ descriptif des opérations de sensibilisation, accompagné des références des intervenants et d'une description de la matière de sensibilisation (documents/maquettes, …) qui sera utilisée,
- ✓ le calendrier global d'exécution, spécifiant clairement toutes les phases d'exécution, accompagné des modèles de l'Annexe 4 y afférents, remplis avec précision,
- ✓ CVs et références de l'équipe d'audit proposée, conformément au modèle fourni en Annexe 5, accompagnés de toutes les pièces justificatives nécessaires,
- ✓ présentation des Outils techniques utilisés, conformément au modèle fourni en Annexe 6.

L'Enveloppe B : doit porter la mention « **Offre Financière** » et contenir :

- ✓ La Soumission conformément au modèle figurant dans le cahier des charges dûment complété de la proposition (selon le modèle fourni dans **l'Annexe 9**;

- ✓ Le tableau du détail des prix (selon le modèle fourni dans **l'Annexe 8**).

Les offres doivent être rédigées en langue française. Toutes les pages des documents exigés dans le dossier technique doivent être datées, signées et comporter le cachet du soumissionnaire.

Article 5 : Ouverture des offres

La commission procèdera à l'ouverture des offres parvenues dans les délais, et vérifiera toutes les pièces demandées sont conformément à l'article 4 du présent cahier des charges.

Le dépouillement des offres sera effectué par une commission désignée à cet effet suivant la méthodologie de dépouillement du Chapitre IV.

Article 6 : Durée de réalisation de la mission

La durée de réalisation de la mission objet du présent cahier des charges, ne doit pas dépasser 45 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 …. « Réception » et des délais d'évaluation du rapport par l'ANSI.

Article 7 : Réception

La réception de la mission d'audit s'effectuera pour la totalité du marché.

Le Maître d'Ouvrage appliquera deux phases de réception :

1- Première phase :

Cette phase consiste en l'approbation par le Maître d'Ouvrage 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 du Maître d'Ouvrage 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 du Maître d'Ouvrage.

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 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) 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, le Maître d'Ouvrage 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, 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 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 8 : 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 au Maître d'Ouvrage, qui notifiera ce fait à tous ceux qui ont retiré le cahier des charges et décidera de la date de la visite. Cette notification sera envoyée au moins quinze (15) 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 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 (annexe 7), cosignée par le visiteur et le responsable du soumissionnaire qui l'aura affecté à cette mission.

Article 9 : 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 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.

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 10 : Modalité de paiement

Le règlement de la valeur des travaux relatifs à cette mission sera effectué comme suit :

- ✓ 20 % (Vingt pour Cent) du montant global du marché payable après l'approbation du rapport détaillé d'audit.

- ✓ 30 % (Trente pour Cent) payable après l'approbation du rapport relatif au plan d'action cadre.

- ✓ 50 % (Cinquante pour Cent) payable après l'approbation du rapport de synthèse et validation de l'étude par l'Agence Nationale de la Sécurité Informatique (ANSI).

Les paiements seront effectués sur présentation de factures établies par l'adjudicataire.

Article 11 : Pénalité de retard

Si les délais prévus par le marché ne sont pas respectés par le titulaire, celui-ci sera passible d'une pénalité de retard calculée à raison de un pour mille (1‰) pour chaque jour de retard sur la valeur du marché objet du retard, sans qu'une mise en demeure préalable ne soit nécessaire. Le montant de la pénalité ne dépassera pas cinq pour cent (5%) du montant global du marché.

Article 12 : Résiliation

Le marché peut être résilié par décision de l'O.D.S aux torts du titulaire dans le cas où :

- ✓ Le titulaire déclare ne pas pouvoir exécuter ses engagements sans qu'il puisse invoquer un cas de force majeure, entre autre 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 relatives au secret professionnel.

- ✓ Le titulaire a perturbé de manière très grave la continuité du service du système audité (plus de 4 heures 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 sa mission, 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.
- ✓ 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 du marché et/ou les étapes de sa réalisation.

La résiliation du marché 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 l'O.D.S qu'à des opérations de liquidation de la phase en cours.

Article 13 : Dispositions diverses

Pour tout ce qui n'est pas prévu par le présent cahier des charges, les dispositions du décret n° 2002-3158 du 17/12/2002 portant règlementation des marchés publics et textes subséquents, et le cahier des clauses administratives générales (CCAG) applicable aux marchés d'études resteront applicables.

Chapitre II - 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 au niveau des structures décrites dans l'annexe A.

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 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 cinq phases. Les phases numérotées de I jusqu'à IV sont 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 l'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, entre autres la fourniture des rapports résultants du dernier audit réalisé.

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 maître d'ouvrage et titulaire,
- ✓ fourniture des détails complémentaires, relatifs au périmètre de l'audit (si le titulaire du marché 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 des documents requis pour l'audit (manuels d'exploitation, schémas d'architectures, politique de sécurité, …),

- ✓ examen des détails des listes des interviews à réaliser par le titulaire et fourniture par le maître d'ouvrage 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.

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.

II - Préparation des activités d'audit :

A. Sensibilisation pré-audit :

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 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.

Le soumissionnaire devrait inclure dans son offre, la réalisation de deux (02) sessions de sensibilisation préliminaires.

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

B. Revue des documents :

Cette phase permettra de déterminer la conformité des documents existants aux exigences de la norme ISO/IEC 27002, d'arrêter la liste des documents manquants exigés par cette norme et d'examiner les problèmes éventuels relatifs à la mise à jour de la documentation.
Plus précisément, l'auditeur doit vérifier si :

- l'information contenue dans les documents fournis est :
  - ✓ Complète (tout le contenu attendu figure dans le document),
  - ✓ Correcte (le contenu est conforme à d'autres sources fiables telles que les normes et les règlements),
  - ✓ Cohérente (le document est cohérent en soi et avec les documents associés),
  - ✓ D'actualité (le contenu est à jour).
- les documents en cours de revue couvrent le périmètre de l'audit et fournissent des informations suffisantes pour appuyer les objectifs de l'audit.

III - Conduite des activités d'audit :

C'est la phase d'audit proprement dite. Elle ne peut commencer qu'après l'achèvement de la revue des documents. Au fur et à mesure de l'avancement dans cette phase, l'auditeur doit vérifier la conformité des procédures opérationnelles avec celles figurant dans les documents fournis.

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 soumissionnaire 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, ..) et de non répudiation).
- ✓ évaluer 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, ….).

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 maître d'ouvrage). 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

Lors des audits, l'utilisation d'outils commerciaux devra être accompagnée de la présentation d'une copie de la licence originale et nominative, permettant leur usage correct pour de telles missions (inexistence de restrictions quant à leur usage pour les audits : plages d'adresses ouvertes, ...).

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) devront 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 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,….),
- ✓ outils de scan d'existence de connexions dial-up dangereuses (war-dialing),

et tout autre type d'outil, recensé nécessaire, relativement aux spécificités du système d'information audité (test d'infrastructure de PKI, ….).

Le soumissionnaire devra donner 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, le lieu (phase de l'audit) et les types de fonctionnalités de l'outil ou script qui seront mises en œuvre (Voir modèle en annexe 5).

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 au commanditaire de l'audit 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.

V - Sensibilisation post-audit :

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

Les sessions post audit, incluant les responsables et acteurs du système d'information, auront pour objectif une sensibilisation aux failles décelées et aux risques cachés encourus et 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.

Le soumissionnaire devrait inclure dans son offre, la réalisation de [nombre de sessions] sessions de sensibilisation post-audit.

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

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. Le Maître d'Ouvrage 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, incluant un résumé des corrections de volumétrie proposées par rapport à l'estimation préliminaire proposée dans le cahier des charges (annexe 3),
- ✓ 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 du Maître d'Ouvrage (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 selon le modèle présenté en annexe 10.

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'évaluation des mesures qui ont été adoptées depuis le dernier audit réalisé et aux insuffisances enregistrées dans l'application de ses recommandations, avec un report des raisons invoquées par les responsables du système d'information et celles constatées, expliquant ces insuffisances,

b) 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,

c) 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,

d) 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,

e) 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,

Les captures d'écran, les résultats de l'exécution des différents outils de l'audit technique ne doivent pas figurer dans le rapport détaillé mais plutôt dans une annexe à part.

Chapitre III - METHODOLOGIE DE DEPOUILLEMENT

Article 1 : 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 nombre d'intervenants est de deux (02) 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 cinq (05) ans,
5. le chef de projet doit avoir piloté au moins trois (03) 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 trois (03) ans,
7. chaque membre de l'équipe intervenante doit avoir participé à au moins deux (02) 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 : Critères d'évaluation

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,
- ✓ La commission de dépouillement procèdera à l'examen de la véracité des documents constituant l'offre financière puis elle fera le classement financier des offres du moins disant au plus disant.

- ✓ La commission procèdera au dépouillement de l'offre technique ayant présenté l'offre la moins disante. Si l'offre technique est conforme aux spécifications demandées, l'offre sera retenue. Si l'offre technique n'est pas conforme aux spécifications demandées, la commission adoptera la même méthodologie avec les offres techniques concurrentes selon le classement financier.

Chapitre IV - ANNEXES

Annexe A1 : Description Technique des systèmes à auditer :

I : Siège de l'ODS à Médenine

Le réseau LAN

- Le réseau actuel de l'ODS est installé au niveau de son siège social à Médenine. Il est composé de **7 serveurs** (un serveur principal composé en trois VMs un de domaine et un de messagerie local @ods.tun , un serveur Antivirus), 2 serveurs d'application) , 1 serveur de sauvegarde et 1 serveur WSUS

et d'une soixantaine de postes de travail .

Le réseau de l'O.D.S est basé sur un Réseau Local fonctionnant sous la plateforme Windows Serveur.

La Salle des Serveurs

Le local technique physiquement sécurisé compte les Serveurs suivants :

- **Un serveur de domaine**
- **Un serveur de messagerie Local (Exchange 2016):**
- **Un Antivirus Kaspersky :**
- **2 serveurs d'Application (SQL Server) :**
- **1 serveur de sauvegarde**
- **1 serveur WSUS**

L'Armoire informatique contient :

- ✓ Quatre Switchs Fortinet
- ✓ Un roteur Tunisie Télécom pour liaison Internet –ODS-ATI Fibre Optique 20 MO
- ✓ Un onduleur.

Les Postes de Travail :

- 60 Postes de travail connectés au réseau local et à l'Internet, Ondulés et protégés par l'Antivirus Symantec gérés par le serveur Antivirus. Fonctionnant sous Windows 7 Pro et Windows 8 Pro.

Quelques Indicateurs d'utilisation de l'informatiques

- ✓ Tous les postes sont connectés au réseau local → 100 % ;
- ✓ Tous le personnel du siège possède un PC -→ 100%.
- ✓ Une connexion Internet Fibre Optique 8 MO Réseau ODS-ATI;
- ✓ Tous les postes sont connectés à Internet 24/24-7/7 ;
- ✓ Tous les utilisateurs possèdent un compte Mail Local @ods.tun → 100% ;
- ✓ Tous les cadres possèdent un compte Mail Officiel (sous ATI) @mdci.gov.tn

Les applications de gestions :

- ✓ Gestion des ressources humaines ;
- ✓ Gestion budgétaires ;
- ✓ Gestion de la trésorerie ;
- ✓ Gestion du bureau d'ordre central ;
- ✓ Gestion de la comptabilité ;
- ✓ Gestion du stock ;
- ✓ Gestion de matériel roulant ;
- ✓ Gestion du carburant ;

Le site web de l'ODS : www.ods.nat.tn

Le site web de l'ODS est hébergé auprès du fournisseur d'accès HEXABYTE , il est en trois langue , à savoir ,l'Arabe , le Français et l'Anglais et actualisé via connexion FTP

II : Six (06) directions régionales

(Directions Régionales de Développement « DRDs ») (Tataouine, Gabes, Kebili, Tozeur, Gafsa, Médenine le même site que le siège).

- ✓ Une connexion Internet Haut Débit (2MO) en ADSL pour chaque Direction Régionale;
- ✓ une connexion VPN entre le siège et les DRDs ;
- ✓ Un réseau local au niveau des DRDs (câblage avec Switch 24 ports mais sans Serveurs central);
- ✓ Le système d'exploitation dominant est Windows 7 et 8 ;
- ✓ Les applications métiers se limitent à la suite bureautique et connexion internet;

Au niveau des Directions Régionales, 40 Micro-ordinateurs répartis comme suit :

- ✓ DRD de Tataouine : 7 Pc de Bureaux ;
- ✓ DRD de Gabes : 9 Pc de Bureaux ;
- ✓ DRD de Kebili : 7 Pc de Bureaux ;
- ✓ DRD de Tozeur : 8 Pc de Bureaux ;
- ✓ DRD de Gafsa : 9 Pc de Bureaux.

Annexe A2 : Présentation de l'Office de Développement du Sud

Création

L'O.D.S., créé depuis 1984 (et restructuré en 1994) est un établissement public à caractère non administratif. Il revient à la tutelle du Ministère du Développement, de l'Investissement et de la Coopération Internationale. Son Siège est à Médenine, la zone d'intervention de l'ODS couvre les Six Gouvernorats du Sud (Tataouine, Médenine, Gabès, Kébili, Tozeur et Gafsa).

Attributions

- ✓ Réunir toutes les informations utiles, procéder aux études nécessaires, proposer toutes mesures pouvant aider dans la définition des politiques en matières de développement en général, de choix des programmes d'investissement public, d'impulsion de l'investissement privé et de l'évaluation des résultats.
- ✓ Assister les autorités régionales dans la conception, l'élaboration et l'exécution des plans et programmes de développement.
- ✓ Elaborer des plans et des programmes complémentaires dans le but de promouvoir et de développer les zones ayant des problématiques spécifiques.
- ✓ Participer à l'élaboration des plans et des programmes d'action visant à promouvoir et à dynamiser l'investissement privé dans les zones concernées, ainsi que le suivi des étapes de leur exécution et ce, en collaboration avec les structures techniques, les

services régionaux spécialisés et les collectivités publiques locales.

- ✓ Soutenir l'action des structures régionales spécialisées et des collectivités publiques locales en matière de promotion de l'investissement privé dans les zones d'intervention.

Zone d'intervention

Les zones d'intervention de l'Office de Développement du Sud sont les gouvernorats de Medenine, Tataouine, Gabes, Touzeur, Gafsa, Kibili.

Organigramme :

Outre la direction générale, l'organigramme de l'O.D.S comprend :

- Direction des Services Communs,
- Direction de l'Informatique et de la Documentation,
- Direction de la Promotion de l'Investissement Privé,
- Direction de la Planification et des Statistiques,
- Direction de l'Appui au Développement et de l'Evaluation, et Coordination des Projets de Coopération,
- Un Guichet Unique groupant des représentants des principaux services pour la création des projets et la constitution des Sociétés,
- Audit interne et contrôle de gestion
- Cellule de gouvernance
- Et six Directions Régionales de Développement aux six Gouvernorats respectifs à savoir : Tataouine, Médenine, Gabes, Kebili, Tozeur et Gafsa.

Le personnel de l'O.D.S est au nombre de 149 dont 61 cadres supérieurs (soit un taux d'encadrement de 40,9%), et 75 agents et cadres travaillant aux directions régionales de développement.

ANNEXE B : Liste des structures à auditer, via un audit sur terrain

	Structure	Lieu d'implantation (gouvernorat)
1.	Siège Social de l'Office de Développement du Sud	Immeuble ettanmia - Médenine
2.	DRD de Médenine	Immeuble ettanmia – Médenine(le même site que le siège
3.		
4.		
5.		
6.		

Chapitre V : MODELES-TYPES DE PRESENTATION DES OFFRES

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

Annexe 1 : Références du soumissionnaire

Ordre	Sous-critère	Réponse : Année / organisme : description [1]
1	Spécialisation de l'entreprise dans l'activité d'audit sécurité	
2	Spécialisation de l'entreprise dans l'activité de la sécurité Informatique (Intégration, Conseil, formation, ….)	
3	Nombre de missions d'audit sécurité, conformes au décret N° 2004-1250, de plus de 30 Jours, effectuées durant les trois dernières années (2013-2014-2015).	

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

Le Soumissionnaire

(Cachet et signature)

Annexe 2 : Qualité des moyens humains mis à la disposition de la mission

2.1 : Présentation du chef du Projet :

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

2.2 : Présentation des membres de l'équipe :

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

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

Le Soumissionnaire

(Cachet et signature)

Annexe 3 : Méthodologie de conduite du projet

Présentation des éléments de la méthodologie de conduite du projet comme suit :

1. **Périmètre de l'Audit :**

   - Critères d'échantillonnage pour chaque type de composante du système d'information à auditer, le cas échéant

2. **Audit organisationnel & physique :**

   - Inspections à réaliser : types, description et résultats attendus,
   - 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,
   - Echantillon du questionnaire à effectuer,
   - les outils d'accompagnements utilisés pour le traitement des interviews, avec la liste des fonctionnalités et la documentation de chaque outil.

3. **Audit technique:**

   - Méthodologie d'Audit technique, incluant le type et l'objet des tests* à réaliser pour chaque phase de l'audit technique suivant:
     - Audit de l'architecture
     - Audit de la configuration de chaque type de composantes du périmètre de l'audit présentées dans l'annexe A (Description volumétrique des structures à auditer)
     - Audit intrusif.
   - Outils utilisés pour réaliser les tests pour chacune des phases de l'audit technique suscitées (voir Annexe 6 : présentation des outils techniques utilisés),
   - La méthodologie d'analyse et de report des failles, selon leur gravité.

4. **Analyse et évaluation des risques:**

   - Méthodologie d'Analyse et d'évaluation des risques, en précisant :
     - les critères de choix de la portée de l'analyse et de l'évaluation des risques,
     - les références d'adéquation de cette méthodologie avec les normes et les méthodologies connues à l'échelle internationale dans le domaine,
   - les outils d'accompagnement pour effectuer l'analyse et l'évaluation des risques.

* pour chaque type de test à réaliser, indiquer les conditions requises pour sa réalisation et les conséquences possibles sur la sécurité et la performance de l'objet du test.

5. Livrables de l'Audit :

- Structure de chaque livrable de l'audit (voir Article 4 du Cahier des Clause Techniques Particulières sur les livrables de l'Audit),
- Modèle de présentation du système d'information existant, et du périmètre de l'audit, qui comprend au moins les éléments décrits au niveau de l'Annexe A (Description volumétrique des structures à auditer),
- Modèle de présentation des résultats de l'Audit pour chaque phase de l'audit et composante du périmètre de l'audit, qui comprend au moins les éléments suivants :
    - Contrôle audité (selon la méthodologie adoptée), constat de l'audit, degré de conformité par rapport au standard utilisé, conséquences possibles engendrées par l'utilisation des vulnérabilités enregistrées, recommandations correspondantes, inspections réalisées pour dégager ces constats, preuves de vérification,
    - Modèle de présentation de la synthèse des vulnérabilités enregistrées, qui comprend au moins les éléments suivants : Description de la vulnérabilité, portée, niveau du risque engendré par l'utilisation de cette vulnérabilité (en faisant sortir les éléments suivants : impact, menace, probabilité d'occurrence, etc), recommandations adéquates,
    - Modèle de présentation du plan d'action.

Annexe 4 : Planning prévisionnel de la mission

Composant		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 5 : Modèle type des CVs Individuels

Nom :	Prénom:

Date de naissance:	Nationalité:

Formation:

Etablissement	
Date: de (mois/année) à (mois/année)	
Diplômes obtenus:	

Formation professionnelle spécifique et certification dans les trois 3 ans (2013-2014-2015):

Organisme	Date	Description

Expérience professionnelle:

Date: de (mois/année) à (mois/année)	
Pays ou ville	
Société	
Poste	
Description	

Date: de (mois/année) à (mois/année)	
Pays ou ville	
Société	
Poste	
Description	

Le Soumissionnaire

(Cachet et signature)

Annexe 6 : Présentation des outils techniques utilisés

- Outils de ……1 :

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

Le Soumissionnaire

(Cachet et signature)

[1]Mettre l'ensemble des types d'outils mentionnés lors de la phase IV- Conduite des activités d'audit du Cahier de Clauses Techniques Particulières.

ANNEXE 7

Annexe 7 : Déclaration sur l'honneur de confidentialité

(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)

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)

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)

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 8 : Modèle de bordereau de prix

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

Soumissionnaire :……..

Désignation	Nombre d'hommes/jours	P.U. HTVA	P.T HTVA	Taux de la TVA	Montant de la TVA	P.T TTC
Mission d'audit de sécurité du système d'information de l'Office de Développement du SUD(ODS)						

Le Soumissionnaire

(Cachet et signature)

Annexe 09 : Modèle de soumission

Je soussigné (Nom, Prénom et Qualité) …….agissant au nom et pour le compte de la Société ……. Sis à ……..……. inscrit au registre de commerce …… et affilié à la Caisse Nationale de Sécurité Sociale sous le n° ……

Après avoir pris connaissance de toutes les pièces du dossier afférent à l'objet de la Consultation lancée par l'Office de Développement du Sud pour un audit de sécurité du système d'information et de communication , reconnaît la nature et l'importance des prestations à exécuter dans le cadre du marché pour lequel je me porte concurrent.

J'arrête le montant de ma soumission financière à :

…… (T.H.T.).

……. (T.T.C.).

Je m'engage à exécuter le marché conformément aux clauses et aux conditions énoncées au cahier des charges en respectant le délai de réalisation et moyennant les prix établis par moi-même que j'ai adressé après avoir apprécié à mon point de vue et sous mon entière responsabilité la nature et l'importance des prestations à exécuter.

En cas d'attribution de la consultation, je m'engage à achever la totalité de travaux objet de la consultation conformément aux détails prescrits dans le cahier des charges dans un délai détaillé selon le planning d'exécution joint dans mon offre technique.

J'accepte le caractère ferme et non révisable de cette consultation.

Je m'engage à rester lié par mon offre pendant la durée de Quatre Vingt Dix (90) jours.

Le maître d'œuvre se libérera des sommes dues par lui en faisant donner crédit au compte ouvert à mon nom ……
…….

Date :

……..

Le Soumissionnaire (Lu et approuvé)

Cachet et signature

Annexe 10 : Description du système 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.