إحصائيات تونس
STATISTIQUES TUNISIE

REPUBLIQUE TUNISIENNE
MINISTERE DE L'ECONOMIE ET DE LA PLANIFICATION
INSTITUT NATIONAL DE LA STATISTIQUE

CONSULTATION N°12 /2025

Mission d'Audit réglementaire

Tri-Annuelle

CAHIER DES CHARGES

Décembre 2025

الجمهورية التونسية
المعهد الوطني للإحصاء

Partie I : Les clauses administratives

Article 1: Objet de la consultation

La présente consultation a pour objet la sélection d'un cabinet d'audit et de consulting en sécurité informatique (avec la possibilité d'avoir un partenaire, dans le cadre d'un groupement) pour la réalisation de l'audit réglementaire de la sécurité informatique de l'Institut National de la Statistique (INS).

Les cabinets intéressés par cette consultation peuvent retirés gratuitement le dossier de la consultation via la plateforme d'achat en ligne « **TUNEPS** » à l'adresse suivante www.tuneps.tn.

Article 2: Documents de la consultation

Le dossier de la présente consultation est constitué par les pièces suivantes :

1. Le présent cahier des charges,
2. La soumission vérifiée sur la base du bordereau des prix,
3. Le bordereau des prix,
4. Le contrat objet de la consultation.

En cas de contradiction ou de différence entre les pièces constitutives de la consultation, ces pièces prévalent dans l'ordre dans lequel elles sont énumérées ci-dessus.

Article 3: Mode de Présentation de l'offre

Le soumissionnaire devra fournir une offre détaillée conformément aux stipulations du cahier des clauses techniques particulières ci-après. Les documents administratifs, l'offre technique et l'offre financière doivent être envoyé à travers le système d'achat en ligne « **TUNEPS** ».

Toutefois l'extrait du registre national des entreprises et la caution bancaire provisoire doivent être envoyées par courrier recommandé ou par rapide poste à l'INS ou remises directement au bureau d'ordre central de l'INS à l'adresse suivante

L'Institut National de la Statistique, 70 RUE Ech-Cham 1002 Tunis BELVIDERE

(Portant la mention ne pas ouvrir et le numéro de la consultation)

La date limite de réception des offres est fixée pour **le 02 Fevrier 2026 à 10 h du matin.**

La participation à travers la procédure en ligne « **TUNEPS** » sera fermée automatiquement le même jour et la même heure. La séance d'ouverture, elle aura lieu **le 02 Fevrier 2026 à 11 h du matin.**

Toute offre parvenue ou reçue en dehors du système « **TUNEPS** » ou après la date limite de réception des offres, sera éliminée.

Chaque soumissionnaire devra accompagner son offre par les documents administratifs et financiers suivants :

1. Une copie d'attestation de dépôt du cahier des charges pour l'exercice de l'activité d'audit en cours de validité, « نسخة من شهادة إيداع كراس شروط لممارسة نشاط التدقيق في مجال السلامة المعلوماتية »
2. La déclaration trimestrielle des salariés et des salaires de la CNSS du dernier trimestre avant la date limite de remise des offres, des auditeurs membres de l'équipe intervenante et employés à temps plein par le soumissionnaire,
3. L'enveloppe contenant le dossier technique doit comporter les pièces suivantes :
   - ✓ Le cahier des charges et ses annexes avec paraphe et cachet humide au bas de chaque page. La signature de la dernière page doit être précédée de la date et de la mention manuscrite « Lu et approuvé »,
   - ✓ Un aperçu succinct sur l'activité générale du soumissionnaire, son organisation et son expérience dans le domaine,
   - ✓ Présentation des références du soumissionnaire (selon le modèle fourni dans l'**Annexe 1**),
   - ✓ Présentation de l'équipe intervenante (selon le modèle fourni dans l'**Annexe 2**),
   - ✓ Méthodologie(s) proposée(s) pour la conduite de l'audit incluant la spécification des outils logiciels d'accompagnement (traitement des enquêtes et calcul de risque) conforme au référentiel établi par l'ANCS (selon le modèle fourni dans l'**Annexe 3**),
   - ✓ 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**.

4. 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**).
5. Le bordereau des prix dûment rempli en chiffres et en toutes lettres datées et portant le cachet du soumissionnaire, conformément au modèle joint en **annexe 8**.

Article 4: Validité des offres

L'offre doit rester valable pendant une durée de **120 jours** après la date limite de réception des offres.

Article 5: Evaluation des offres

C'est la commission interne des achats qui procède à la vérification et l'évaluation des offres.

Article 6: Complément d'information

Au cas où certains soumissionnaires auraient des renseignements à demander ou auraient des doutes sur la signification exacte de certaines parties des documents de la consultation, ils devraient en référer par écrit, à l'INS en vue d'obtenir les éclaircissements nécessaires avant de transmettre leurs offres, cinq (05) jours au plus tard avant la date limite de réception des offres.

Si les questions sont fondées, elles feront l'objet d'additifs au dossier de la consultation lesquels seront, transmis à tous ceux qui ont retiré le dosser cinq (05) jours au plus tard avant la date limite de réception des offres. Ces additifs feront partie des documents de la consultation.

Aucune réponse ne sera apportée à des questions verbales et toutes interprétation par un soumissionnaire des documents de la consultation, n'ayant pas fait l'objet d'un additif sera rejetée et ne pourra pas impliquer la responsabilité du l'INS.

Article 7: Le cautionnement provisoire

Toute offre doit contenir obligatoirement une caution bancaire provisoire et payable à première demande de l'INS sans recours à aucune formalité administrative, **sept cent cinquante (750) dinars**.

La caution provisoire est valable pendant une période de cent vingt (120) jours à partir du lendemain du jour du dernier délai de réception des offres.

Article 8: La caution définitive

Dès la signature du contrat de la consultation, le titulaire doit remplacer la caution provisoire par une caution définitive dans un délai ne dépassant pas les vingt (20) jours.

Le montant du cautionnement définitif ne peut être supérieur à trois pour cent (3%) du montant total de la consultation.

Le cautionnement définitif est restitué au titulaire de la consultation, à l'expiration du délai d'un mois à compter de la date de réception définitive des prestations objet de la consultation, à condition que le titulaire se soit acquitté de toutes ses obligations.

Article 9: Eclaircissements

En vue de faciliter l'examen, l'évaluation et la comparaison des offres, l'INS a toute la latitude de demander au soumissionnaire de donner des éclaircissements sur son offre notamment des justificatifs concernant les informations fournies. Cette demande se fera par écrit ainsi que la réponse. Toutefois, en aucun cas ces éclaircissements ne doivent avoir une incidence sur le montant ou la teneur de la soumission.

Article10: Le Contrat objet de la consultation

Le contrat de cette consultation n'entrera pas en vigueur qu'après sa signature par les deux parties.

Article11: Enregistrement du Contrat

Les frais d'enregistrement et le timbre fiscal du contrat résultant de la présente consultation sont à la charge du titulaire, qui doit remettre un exemplaire enregistré à l'INS.

Article12: Variation dans le volume

En cas d'augmentation ou de diminution dans le volume des prestations, le titulaire de la consultation ne peut élever aucune réclamation ou réserve tant que cette augmentation ou diminution n'excède pas 20% du montant total de la consultation.

Article13: Licences et Brevets

Le titulaire garantira l'INS contre toute réclamation des tiers touchant à la contrefaçon ou à l'exploitation d'un brevet, d'une marque commerciale ou de droit de création résultant de l'emploi de logiciels, des fournitures ou de leurs composants.

Article14: Paiement

Le paiement sera effectué après la fin de chaque mission annuelle et après la validation du rapport final par l'Agence Nationale de la Cybersécurité (ANCS). Suite à la réception de la facture finale.

Article15: Délais

Le délai de réalisation de la présente consultation ne doit pas dépasser **02 mois** à partir de la date de commencement des travaux définis dans un PV de lancement de la mission signé par les deux parties contractantes.

Article 16: Pénalité de retard

Si les délais prévus ne sont pas respectés (sauf en cas de force majeure mentionné), par le titulaire sera passible d'une pénalité calculée à raison de 1/1000 (un pour mille) pour chaque jour de retard sur la valeur de la mission, sans qu'une mise en demeure préalable ne soit nécessaire. Le montant de cette pénalité ne dépassera pas 5% du montant total de la consultation

Les retards dus à l'INS et dument justifiés par le titulaire, dans l'exécution d'une mission s'ajouteront aux délais relatifs à cette même mission.

Article 17: En cas de refus de l'Audit par l'ANCS

Si le rapport d'audit est refusé par l'Agence Nationale de la Cybersécurité, le titulaire est tenu de procéder à ses frais, à la correction des manquements signalés.

Article 18: Résiliation de la consultation

➢ **Résiliation par l'INS**

La consultation sera résiliée par décision de l'INS 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.
- La qualité des prestations fournies par le titulaire s'avéré non satisfaisante (qualité non satisfaisante des livrables, non-respect des délais……) compte tenu des pratiques professionnelles, des règles de l'art et des exigences du cahier des charges.
- Le titulaire viole les dispositions relatives au secret professionnel.
- Le titulaire perturbe de manière très grave la continuité du service, en ayant procédé à des tests connus pour être risqués, sans préavis et autorisation préalable.
- Le titulaire accumule des retards supérieurs à 30 jours calendaires par rapport au planning convenu.

La résiliation 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.

➢ **Résiliation par le titulaire**

La consultation peut être résilié par décision du titulaire aux torts de l'INS dans le cas où :

L'INS déclare ne pas pouvoir exécuter ses engagements sans qu'elle puisse invoquer un cas de force majeure. La résiliation ne fera pas obstacle à la mise en œuvre des actions civiles ou pénales qui pourraient être intentées contre l'INS en raison de ses fautes.

Article 19: Sous Traitance

Le titulaire ne peut recourir à la sous-traitance pour l'exécution de cette mission sans l'accord préalable de l'INS.

Il ne peut ni en faire apport à une société ni en confier l'exécution totale ou partielle à un ou plusieurs sous-traitants sans l'autorisation préalable de l'INS. Dans tous les cas, le titulaire doit assurer sous son entière responsabilité toutes les missions afférentes à cette consultation. A ce titre il demeure le seul responsable de la bonne exécution de cette mission.

Article 20: Clauses de confidentialité

Le titulaire s'engage :

- A ne pas lister dans une liste de références l'INS, sans accord explicite de celle-ci
- A ne pas divulguer aucune information concernant les mesures de sécurité prises par l'INS,
- A faire signer une clause de confidentialité par tous les intervenants au sujet des plans et mesures de sécurité mises en place par l'INS qui lui ont été transmises ou dont il a eu connaissance au cours de l'exécution de cette mission.

Article 21: Listes des Intervenants et pièces d'identités

Le titulaire devra transmettre une copie des pièces d'identités des intervenants.

Toute modification dans la liste des intervenants doit être communiquée à l'INS au moins 72 heures à l'avance, l'INS peut écarter certains intervenants proposés par le titulaire.

Article 22: Annulation de la consultation

L'INS peut annuler la consultation pour des motifs techniques ou financiers. Les candidats en sont informés

Article 23: La force majeure

Conformément aux articles 282 et 283 du code des obligations et des contrats, le terme « force majeure » désigne un événement échappant au contrôle du soumissionnaire et qui n'est pas attribuable à sa faute ou à sa négligence et qui est imprévisible.

De tels événements peuvent inclure les guerres, les révolutions, les inondations, les épidémies, les mesures de quarantaine et d'embargo sur le fret.

En cas d'événement lié à la force majeure, le soumissionnaire notifiera à l'INS l'existence de la force majeure et ses motifs et s'efforcera de trouver tout autre moyen d'exécuter les obligations dont l'exécution n'est pas entravée par la force majeure.

Article 24: Règlement des litiges

Les litiges qui pourraient découler de l'interprétation ou de l'exécution des clauses de la présente consultation seront, résolus à amiable entre les deux parties, si le différend persiste encore, les deux parties font recours aux tribunaux compétents de Tunis conformément à la réglementation en vigueur.

Article 25: Cadre juridique et disposition règlementaires

La consultation sera régie par la réglementation Tunisienne en vigueur et tous les textes qui la complètent. Pour tout ce qui n'est pas prévu dans le présent cahier des charges.

FAIT à ..... Le, ...

Cachet et signature du soumissionnaire

PARTIE II Cahier des clauses Techniques

Partie II : Les clauses techniques

Objectifs de la consultation

L'institut National de la Statistique (**INS**) 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-loi 2023-17 du 11 mars 2023, à l'arrêté applicatif du ministre des technologies de la communication du 12 septembre 2023, fixant les critères techniques d'audit et les modalités de suivi de la mise en œuvre des recommandations contenues dans le rapport d'audit ainsi qu'aux dispositions du présent cahier des charges et ce, pour une durée d'un (1) an renouvelable par tacite reconduction avec une durée maximale de trois (3) ans.

L'annexe A1 présente un aperçu sur le « Système d'information » de l'INS.

1- Définitions et interprétations

Maître d'Ouvrage	Désigne l'**INS** et 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 droits légaux dudit prestataire.
Mission	Signifie toute action d'audit, de test, de vérification y compris la rédaction des rapports, les déplacements, la collecte de données, l'analyse des tests, et toute autre action assurée par le titulaire pour le compte du Maître d'Ouvrage dans le cadre de la bonne exécution 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.
ANCS	Désigne l'Agence Nationale de la Cyber Sécurité.

2- Conditions de participation

Cette consultation s'adresse aux experts auditeurs, personnes physiques ou morales, habilités à exercer l'audit dans le domaine de la cyber sécurité conformément au décret-loi 2023-17 du 11 mars 2023 et à l'arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité de l'information. (La liste actualisée est disponible sur le site web www.ancs.tn).

La procédure de soumission des offres doit être en ligne via le système national des achats publics en ligne TUNEPS.

3- Présentation de l'offre

L'offre est constituée de :

- L'offre technique,
- L'offre financière.

Est admis à soumissionner tout fournisseur qui possède toutes les garanties requises pour assurer dans de bonnes conditions l'exécution de la présente consultation.

Les personnes physiques ou morales en état de faillite ne sont pas admises à soumissionner.

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.

4- 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 respecter le modèle de rapport d'audit établi par l'ANCS (Modèle de rapport d'audit).

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

1. 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,
2. 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,
3. De la qualité des résultats (estimation des risques, ...) issus des travaux d'audit et de leur complétude,
4. De la qualité des recommandations émises,
5. 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) :

6. De la qualité et complétude des livrables fournis,
7. De la qualité (pertinence, pragmatisme) des recommandations issues des travaux d'audit et de leur complétude,
8. 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'ANCS ou de la commission d'arbitrage énoncée dans la réglementation des marchés publics ou d'un expert habilité à exercer l'activité d'audit dans le domaine de la cyber sécurité, 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.

5- Mission 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 doit figurer parmi les experts de l'entreprise mentionnés au niveau de la liste des personnes physiques ou morales autorisées à exercer l'activité d'audit dans le domaine de la cyber sécurité sur le site web www.ancs.tn.

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.

6- 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, quel que 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.

CAHIER DES CLAUSES

TECHNIQUES PARTICULIERES

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.

Cet audit devra se conformer, au minimum, aux dispositions énoncées dans le décret-loi 2023-17 du 11 mars 2023 et l'arrêté applicatif du ministre des Technologies de la communication du 12 septembre 2023, fixant les critères techniques d'audit et les modalités de suivi de la mise en œuvre des recommandations contenues dans le rapport d'audit. En plus, il doit être réalisé par un expert auditeur, personne physique ou morale, habilités à exercer l'activité d'audit dans le domaine de la cyber sécurité conformément à l'arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité de l'information (la liste actualisée est disponible sur le site web www.ancs.tn).

Cet audit devra suivre une approche méthodologique conforme au référentiel établi par l'ANCS qui couvre les aspects organisationnels, physiques et opérationnels relatifs à la sécurité du système d'information inclus dans le périmètre de cet audit.

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, ISO27001 et ISO27002.

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, côté 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 autres, 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 **03 sessions de sensibilisation préliminaires** d'une demi-journée.

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 recommandations de la norme ISO/IEC 27002, d'arrêter la liste des documents manquants 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.

Aussi, est-il opportun d'examiner les documents relatifs à la mise en œuvre des recommandations émises dans le rapport de l'audit précédent ainsi que tout document issu d'autres audits éventuels.

Il convient d'accorder une attention particulière à cette phase compte tenu de l'importance que revêt la documentation dans le bon déroulement des activités de l'organisme indépendamment des personnes. Aussi faut-il tenir compte, durant cette phase, de la taille, de la nature et de la complexité de l'organisme.

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 préétablis 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.

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 cette 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 :
    a. 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,
    b. 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 03 sessions de sensibilisation post-audit d'une demi-journée chacune.

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.

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 respectant le référentiel établi par l'ANCS.

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. 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.

4- Livrables

Le titulaire doit remettre au maitre d'ouvrage :

- ✓ Un rapport d'audit préparé conformément au modèle de rapport d'audit établi par l'ANCS (Modèle de rapport d'audit),
- ✓ Un rapport de synthèse destiné à la direction générale (destiné décideurs).

Ces rapports doivent être datés, visés et porter le cachet de l'expert auditeur. Les captures d'écran et les résultats de l'exécution des différents outils de l'audit technique doivent figurer dans une annexe à part.

Acceptation provisoire : L'acceptation provisoire est prononcée après la validation interne des livrables et la signature d'un procès-verbal (PV) de réception provisoire par les deux parties.

Acceptation définitive : L'acceptation définitive de la prestation d'audit est prononcée après validation du rapport final par l'Agence Nationale de la Cybersécurité et signature du procès-verbal de réception définitive par les deux parties.

METHODOLOGIE DE DEPOUILLEMENT

Article 1er : Critères de conformité technique

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

Les critères de conformité technique sont :

1. Le soumissionnaire est habilité par l'Agence Nationale de la Cyber Sécurité, conformément à l'arrêté du ministre des Technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité de l'information.
2. Le nombre d'intervenants est de 03 personnes au minimum certifiés par l'ANCS, sans compter le chef de projet,
3. Le chef du projet est un auditeur parmi les cadres déclarés dans le cahier des charges pour l'exercice de l'activité d'audit déposé à l'ANCS,
4. L'expérience du chef de projet est supérieure ou égale à 15 ans,
5. Le chef de projet doit avoir piloté au moins 15 missions d'audit de sécurité des systèmes d'information pour le compte d'organismes de taille similaire,
6. Le chef de projet doit détenir les certifications suivantes (au moins 3 parmi 5 certificats sont en cours de validité) :
   - ISO 21502 Senior Lead Project Manager ou PMP ou Prince2
   - ISO 27001 Senior Lead Auditor
   - ISO 27001 Senior Lead Implementer
   - ISO 27005 Senior Lead Risk Manager
   - ISO 22301 Senior Lead Auditor
7. Le chef de projet doit détenir une certification en tant qu'expert auditeur (présent dans la liste des experts auditeurs publiés par l'ANCS
8. L'expérience de chaque membre de l'équipe intervenante est supérieure ou égale 03 ans,

9. Chaque membre de l'équipe intervenante doit avoir participé à au moins 10 missions d'audit de sécurité des systèmes d'information pour le compte d'organismes de taille similaire,
10. Au moins deux (2) membres certifiés ISO 27001 Lead Auditor enter
    - Au moins un (1) membre certifié ISO 27005 Risk Manager
    - Au moins un (1) membre certifié CEH
    - Au moins Deux (2) membres avec une expérience supérieure à 5 ans
11. 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,
- Critères financiers : l'offre la moins disante sera retenue.

Par ailleurs, chaque soumissionnaire doit présenter une offre pour la réalisation des formations certifiantes suivantes en présentiel dans un centre agréé et accrédité par EC COUNCIL et PECB (Spécifier le centre de formation) situé au grand Tunis :

Année	**Nom de la formation Certifiante**
Année 1	Certified SOC Analyst (EC-Council)
	Certified Lead Lead SOC 2 Analyst (PECB)
Année 2	SOC Engineer : COMPTIA SECURITY+
	Computer Hacking Forensic Investigator (EC-council CHFI)
Année 3	CompTIA CySA+
	ISO/IEC 27701 Lead Implementer (PECB)

ANNEXES


الجمهورية التونسية
المعهد
الوطني
للإحصاء
وزارة الإقتصاد والتخطيط

ANNEXE A1

Description Technique des systèmes à auditer :

L'INS dispose d'un site principal – sis au 70 rue Echam - Lafayette, ainsi que d'un site annexe sis au 86 rue Hédi chaker – Lafayette – connecté via Fibre Optique (FO) et backup FO.

L'INS dispose aussi de dix bureaux régionaux connectés via FO et backup ADSL (des réseaux LAN avec un Firewall, une vingtaine de postes de travail ; et un seul serveur pour le partage des fichiers) et 13 bureaux locaux connecté via ADSL (09 postes de travail en moyenne)

1. Un site web hébergé chez l'ATI
2. Le site principal de l'INS :
- Des Serveurs (Hôtes physiques et serveurs virtuels)
- Deux firewalls,
- Des switchs,
- Un contrôleur Wifi
- Des Points d'accès Wifi
- Des telephones IP
- Réseau MPLS,
- Baies de stockage

3. Le site Annexe héberge :
- Deux firewalls,
- Des switchs,
- Des Points d'accès Wifi
- Des telephones IP
- Réseau MPLS…

4. Les dix bureaux régionaux :
- Des switchs,
- Des firewalls,
- Des Points d'accès Wifi
- Des telephones IP
- Réseau MPLS…

La liste détaillée des applications et des équipements est consultable dans les locaux de l'INS et sera communiquée aux soumissionnaires sur simple demande.

ANNEXE A2

Organigramme global des entités à auditer :

(Fournir assez de détails (non confidentiels), relatifs à la structuration des entités à auditer, pour permettre une correcte estimation du planning d'exécution)

.....

.....

.....

ANNEXE B

Liste des structures à auditer, via un audit sur terrain

	Structure	Lieu d'implantation (gouvernorat)
1.	Siège	Tunis
2.	Site Annexe	Tunis
3.	Bureau régional 20 mars	Tunis
4.	Bureau local de Zaghouan	Zaghouan

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 cyber sécurité (Intégration, Conseil, formation, …)	
3	03 de missions d'audit de sécurité réglementaire, conformes à la loi n°2004-5 ou au décret-loi n°2023-17, de plus de 60 Jours, effectuées durant les trois dernières années.	

[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

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]

2.1 : Présentation du chef du Projet :

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.

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 le référentiel d'audit établi par l'ANCS,
   - Echantillon du questionnaire à effectuer,
   - Les outils d'accompagnement 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.

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 :

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	

المعهد الوطني للإحصاء

Société	
Poste	
Description	

ANNEXE 6

Présentation des outils techniques utilisés

- Outils de .....:

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

ANNEXE 7

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE

(Soumissionnaire)

Je soussigné(e) M./Mme ....., Responsable de la société ....., déclare désigner M./Mme ....., Expert(e) auditeur(trice) déclaré(e) à l'Agence Nationale de la Cyber Sécurité et faisant partie de notre société, pour nous représenter lors de la réunion d'éclaircissement relative au contenu du cahier des 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

(Délégué)

Je soussigné(e) M./Mme ....., Expert(e) auditeur(trice) déclaré(e) à l'Agence Nationale de la Cyber Sécurité 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 .....

M./Mme.....,

CIN N° .....

(Cachet de la société et signature)

ANNEXE 8

MODELE DE BORDEREAU DES PRIX **Année 1**

(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.TTTC
Mission d'audit de sécurité du système d'information de l'INS						
Formations certifiantes [1]	01 personne					

Montant total HTVA .....

Dinars Tunisien (en toutes lettres)

TVA (en %) .....

Montant total de la TVA .....

Dinars Tunisien (en toutes lettres)

Montant total TTC .....

Dinars Tunisien (en toutes lettres)

Fait à ....., le .....

Signature et cachet du soumissionnaire

[1] Les formations se réalisent durant la durée, sujet de cette consultation

MODELE DE BORDEREAU DES PRIX **Année 2**

(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.TTTC
Mission d'audit de sécurité du système d'information de l'INS						
Formations certifiantes [1]	01 personne					

Montant total HTVA .....

Dinars Tunisien (en toutes lettres)

TVA (en %) .....

Montant total de la TVA .....

Dinars Tunisien (en toutes lettres)

Montant total TTC .....

Dinars Tunisien (en toutes lettres)

Fait à ....., le .....

Signature et cachet du soumissionnaire

[1] Les formations se réalisent durant la durée, sujet de cette consultation

MODELE DE BORDEREAU DES PRIX **Année 3**

(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.TTTC
Mission d'audit de sécurité du système d'information de l'INS						
Formations certifiantes [1]	01 personne					

Montant total HTVA ..... Dinars Tunisien (en toutes lettres)

TVA (en %) .....

Montant total de la TVA .....

Dinars Tunisien (en toutes lettres)

Montant total TTC .....

Dinars Tunisien (en toutes lettres)

Fait à ....., le .....

Signature et cachet du soumissionnaire

[1] Les formations se réalisent durant la durée, sujet de cette consultation