Tunis le 15 Décembre 2022

Consultation N° 01/2022

TERMES DE REFERENCE POUR L'AUDIT DE LA SECURITE DES SYSTEMES D'INFORMATION DE L'ONMNE

Dernier délai de réception des offres : Vendredi 30 Décembre 2022 à 11 H

5-7, Rue Khartoum, Complexe Diplomat, bloc 4, 13ème étage, Le Belvédère, 1002, Tunis Tel : 71 284 542/547/560/561
Fax : 71 894 533 Email : onmne@rns.tn

CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIERES

Article 1 : Objet de la consultation

L'ONMNE 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 : Définitions et interprétations

Maître d'Ouvrage	désigne l'*ONMNE* 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 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 : Conditions de participation

Cette consultation s'adresse aux experts auditeurs, personnes physiques ou morales, habilités à exercer l'audit de la sécurité informatique conformément à la loi 2004-05 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 informatique. (la liste actualisée est disponible sur le site web www.ansi.tn).

Article 4 : Présentation de l'offre

Le dossier de la soumission doit nécessairement être constitué de l'offre technique et de l'offre financière.

Les offres sont adressées au plus tard vendredi le 30 décembre 2022 à 11H par voie postale et recommandé ou par rapide poste ou par dépôt direct au bureau d'ordre de l'ONMNE (contre un décharge ou un bon de dépôt) sous pli fermé portant la mention « à ne pas ouvrir- Consultation N°01/2022 « AUDIT DE LA SECURITE DES SYSTEMES D'INFORMATION DE L'ONMNE» durant l'horaire administratif à l'adresse suivante :

Observatoire National des Maladies Nouvelles et Emergentes 5/7 Rue Khartoum, Complexe Diplômât bloc4, 13ème étage, Belvédère 1002 Tunis.

Toute offre parvenue après le dernier délai de réception des offres sera rejetée. (Le cachet du BO de l'ONMNE faisant foi).

L'enveloppe extérieure doit contenir :

1. Les pièces administratives,
2. Un 1er pli fermé pour l'offre technique,
3. Un 2eme pli fermé pour l'offre financière.

4.1 Les pièces administratives

L'offre du soumissionnaire doit renfermer l'ensemble des pièces administratives suivantes :

• Une copie d'attestation de dépôt du cahier des charges pour l'exercice de l'activité d'audit déposé à l'ANSI en cours de validité,

" نسخة من شهادة ايداع كراس شروط لممارسة نشاط التدقيق في مجال السلامة المعلوماتية"

• 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,

• 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).

4.2 Offre technique

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'ANSI (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,

• Les 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.

4.3 Offre financière

La deuxième enveloppe contenant l'offre financière doit renfermer les documents suivants établis selon les modèles en annexe :

• Le bordereau des prix en Dinars Tunisiens en hors taxes et toutes taxes comprises selon l'annexe n°8.

N.B : 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 : Durée de réalisation de la mission

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

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

Ce délai ne tient pas compte des délais additionnels éventuels pris pour la correction (validation) des différents livrables exigés dans le présent cahier des charges, et ce conformément à l'article 6 « Réception » et des délais d'évaluation du rapport par l'ANSI.

Article 6 : 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'ANSI (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 :

- 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 habilité à exercer l'activité de l'audit de la sécurité informatique, 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 7 : 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 doit figurer parmi les experts de l'entreprise mentionnés au niveau de la liste des personnes physiques ou morales certifiées par ANSI sur le site web www.ansi.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.

Article 8 : 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 9 : Durée de validité des offres

Tout soumissionnaire sera lié par son offre pendant soixante (60) jours à compter du jour suivant la date limite fixée pour la réception des plis.

Article 10 : Langue de l'offre

L'offre préparée par le soumissionnaire, ainsi que toutes les correspondances, les caractéristiques techniques et toute documentation concernant l'offre, doivent obligatoirement être rédigées en langue française.

Article 11 : Ouverture des plis et Évaluation des offres :

La commission d'ouverture des plis se réunit, une seule fois pour ouvrir les enveloppes contenant l'offre financière et l'offre technique.

La séance d'ouverture des plis n'est pas publique.

Le dépouillement des offres sera fait selon la méthodologie suivante :

La commission d'évaluation procède dans une première étape à la vérification, outre des documents administratifs, de la validité des documents constitutifs de l'offre financière, à la correction des erreurs de calcul le cas échéant et au classement de toutes les offres financières par ordre croissant

Toute erreur de calcul observée sera corrigée et, en cas de différence entre le montant partiel et le montant total, ou entre mots et chiffres, les premiers prévalent.

La commission d'évaluation procède dans une deuxième étape à la vérification de la conformité de l'offre technique du soumissionnaire ayant présenté l'offre financière la moins disante et propose de lui attribuer la consultation en cas de sa conformité aux cahiers des charges.

Si ladite offre technique s'avère non conforme aux cahiers des charges, il sera procédé selon la même méthodologie, pour les offres techniques concurrentes selon leur classement financier croissant.

Article 12 : Règlement des litiges.

Les parties s'efforceront de régler à l'amiable les différends qui pourraient surgir entre elles au sujet de l'interprétation ou de l'exécution du contrat.

A défaut d'accord amiable, tout litige découlant du contrat sera tranché définitivement par le tribunal de première instance de Tunis.

Article 13 : Résiliation du contrat :

Le décès, la dissolution, la faillite et la liquidation judiciaire du fournisseur entraînent de plein droit la résiliation du contrat.

L'ONMNE se réserve le droit de résilier le contrat aussi si le fournisseur ne respecte pas ses obligations contractuelles envers l'administration.

Article 14 : Entrée en vigueur

Le contrat qui sera conclu dans le cadre de cette consultation ne sera valable qu'après sa signature par les deux parties.

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 (voir aussi comme clarifications l'annexe 10 et l'annexe 11).

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 un expert auditeur, personne physique ou morale, habilités à exercer l'audit de la sécurité informatique conformément à la loi 2004-05 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 informatique. . (la liste actualisée est disponible sur le site web www.ansi.tn).

Cet audit devra suivre une approche méthodologique conforme au référentiel établi par l'ANSI qui couvre les aspects organisationnels, physiques et opérationnels 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 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.

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 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.

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 02 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 respectant le référentiel établi par l'ANSI.

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.

Article 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'ANSI (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.

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 habilité par l'Agence Nationale de la Sécurité Informatique, 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 informatique.
2. le nombre d'intervenants est de 02 personnes au minimum, 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'ANSI,
4. l'expérience du chef de projet est supérieure ou égale à 05 ans,
5. le chef de projet doit avoir piloté au moins 05 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 02 ans,
7. chaque membre de l'équipe intervenante doit avoir participé à au moins 05 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 1 : critère de conformité technique) sera éliminée,
- Critères financiers : l'offre la moins disante sera retenue.

ANNEXES

ANNEXE A1

Description Technique des systèmes à auditer :
(Fournir assez de détails (non confidentiels), relatifs aux entités à auditer, pour permettre une correcte évaluation du travail demandé et une bonne formulation des réponses)

(Voir plus de détails en annexe 10)

Et une Architecture synoptique, en omettant les détails compromettants (identité des sites, …)
(Voir plus de détails en annexe 11)

(Les détails complémentaires, de nature jugée très confidentielle, devront être fournis, sous couvert de la stricte confidentialité, lors de la mission de reconnaissance)

Et si possible, fournir une estimation volumétrique, permettant d'aider à évaluer, avec plus de précision, la volumétrie du travail demandé :

Description Volumétrique des structures à auditer (**voir dans l'annexe 10**)

	Volumétrie du Système d'Information	Périmètre de l'audit
Sites à visiter et leur lieu		
Nombre de responsables à interviewer		
Centres de calcul à auditer		
Autres infrastructures spécifiques à auditer physiquement et/ou organisationnellement		
Autre détails particuliers sur le niveau d'inspection physique ou/et organisationnel désiré	**4**	**Audit de sécurité applicatif *.onmne.tn et notamment episurveille.onmne.tn**
PC		
Nb Total de PCs		
Type d'OS :		
- Nombre moyen de PC sous Windows		
- Nombre moyen de PC sous Mac OS		
- Nombre moyen de PC sous Linux		
Autres OS.		
Serveurs		
Nombre Total de Serveurs		
- Type d'OS		
- Nombre d'utilisateurs supportés		
Applications		
Nombre d'applications (objet de l'audit de sécurité)		
- Nombre d'utilisateurs		
- Environnement des applications		
Réseau		
- Nombre de sites distants interconnectés		

- Nombre de sous-réseaux (internes et externes)	04	Boucles/saturations/interférences/Qualités de services/plages d'adresses
- Connexions externes :		
. Nombre de connexions permanentes, leur type (LS, FR,…) et leurs utilisations (Internet, inter-sites, avec des sites externes)		
. Nombre de Connexions Dial-Up et leurs utilisations (Internet, inter-sites, avec des sites externes)		
. Nombre de routeurs et types de connexions supportées		
Nombre de switchs et niveau (2,3,…)		
Outils d'administration réseau et leurs types	rien	**Nous fournir les spécifications(specs) techniques**
Autres : ……		
Outils de Sécurité		
Firewalls		
Nombre de systèmes de Firewalling, leurs types et Nombre de DMZs supportées	**Voir VDOM décrit à l'annexe 10**	01
Type de connexions VPN activées au niveau des firewalls.	Accès vpn backoffice/ftp/database des applications web hebergées à l'ATI	03
Serveurs anti-virus		
Nombre de serveurs anti-virus et nombre de licences	rien	selon vos recommandations
Nombre de passerelles anti-virales et leur usage (e-mail, web, FTP,…	rien	**Nous fournir les specs techniques**
Outils d'authentification		
Nombre de serveurs d'authentification réseau internes et nombre moyen d'utilisateurs supportés	rien	selon vos recommandations
Nombre de serveurs d'authentification réseau pour les accès distants et nombre moyen d'utilisateurs supportés	rien	**Nous fournir les specs techniques**
Outils de détection d'intrusion		
Nombre de NIDS (IDS réseau)	rien	selon vos recommandations
Nombre de sondes HIDS (IDS hôte)	rien	selon vos recommandations
Nombre de Firewalls PC ou Distribués	rien	selon vos recommandations
Outils de sauvegarde automatique et leurs types	rien	**Nous fournir les specs techniques**
Outils intégrés d'administration de la sécurité et leurs types	rien	**Nous fournir les specs techniques**
Autres outils, le cas échéant (authentification forte, PKI, chiffrement, ...)	rien	**Nous fournir les specs techniques**

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.	ONMNE (2 étages= 13ème et 2ème étage)	Tunis

Modèles-types de présentation 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 …. 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

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.

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'ANSI,
   - 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.
   - 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.

3. **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	
Société	
Poste	
Description	

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, ..)

[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

DECLARATION SUR L'HONNEUR DE CONFIDENTIALITE
(Soumissionnaire)

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

Le Soumissionnaire

(Cachet et signature)

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

MODELE DE BORDEREAU DES 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'ONMNE						

ANNEXE 10 : Description Technique des systèmes à auditer

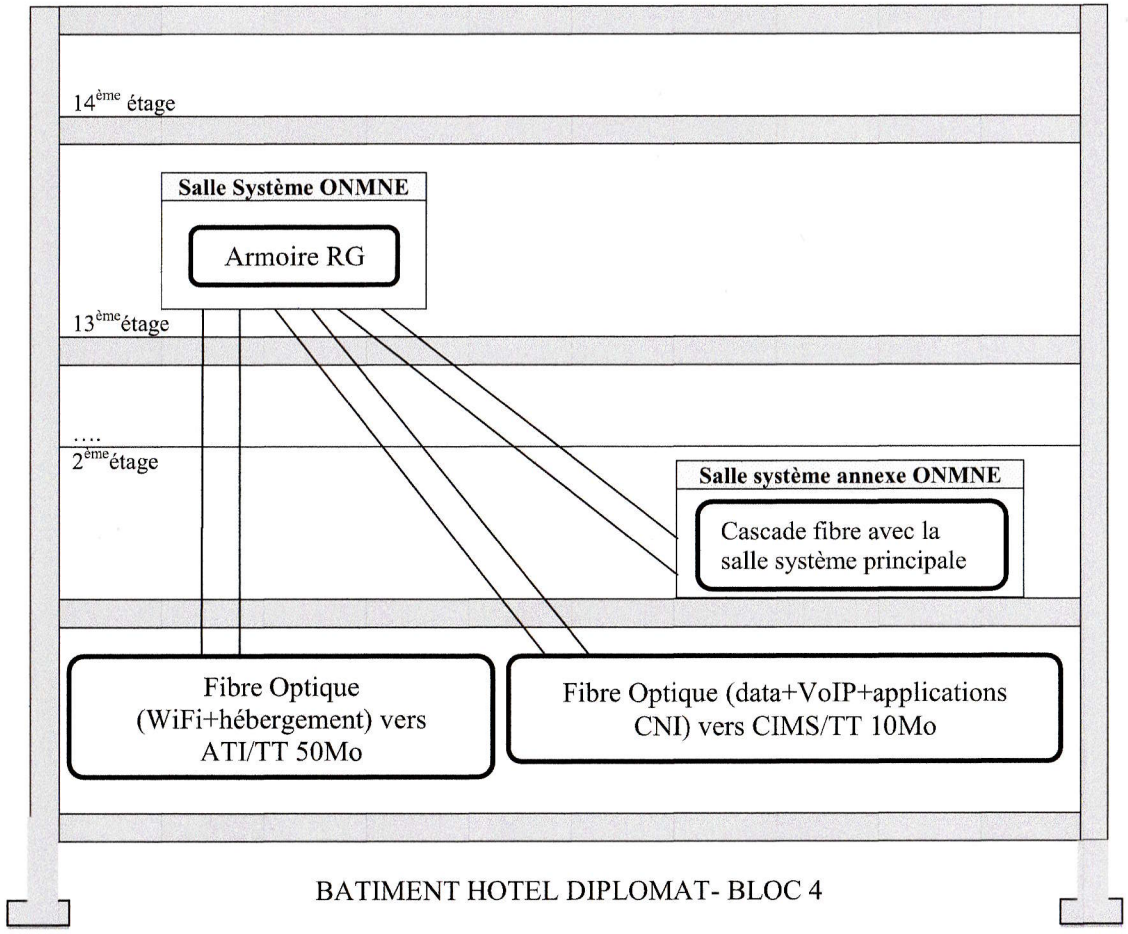
Indicateurs de Volumétrie pour l'audit Organisationnel et physique		
Nombre de sites à visiter	02	
Lieux	5/7 Rue Khartoum complexe Diplômât bloc 4- 13ème étage+2ème étage, Belvédère Tunis 1002	
Nombre de responsables à interviewer	21	
Nbr Total de PCs	35Pcs	
Type d'OS :	Windows XP/Windows 7/Windows 8, Windows 10	
Nombre moyen de PC sous Windows	35	
Nombre moyen de PC sous MacOS	01	
Nombre moyen de PC sous Linux	0	
Autres OS.	-	
Equipements Wifi	13ème étage: 06 points d'accès 2ème étage: 08 points d'accès	
Applications		
	Hébergement	Nombre d'utilisateurs
Site web onmne.tn, messagerie @onmne.tn, application web episurveille.onmne.tn, site application sormas.onmne.tn	ATI	Personnel

Réseau

Nombre de sites distants interconnectés	2
Nombre de sous réseaux (internes)	Site1 : 03 et Site2 : 03

Connexions externes : Nombre de connexions permanentes, (Internet, data et VoIP)	Site1 : 2 liaisons Fibre optique (ATI+CIMS) Site2 : cascade liaison Fibre optique
Nombre de routeurs	02
Nombre de switchs et niveaux (2, 3,)	05 (Site1 : 2 Switch Niv3 et 2 Switch Niv2 Site2 : 02 Switch Niv2
Nombre de postes IP	50
Nombre de VLANs	03(applications CNI/VoIP/WiFi visiteur)
Serveurs internes	
Serveur ftp serv-u installé aux locaux de l'ONMNE	01
Firewall	
Firewall qui ce trouve au POP de l'ATI et dont l'ONMNE a son VDOM et passe a travers un contrôle, gère ou administre son trafic et toute sa sécurité a travers sa session de FortiManager & Fortianalyser	01

ANNEXE 11 : Schéma synoptique du site ONMNE



ANNEXE 12 : Fiche à remplir pour chaque visite sur site effectuée par un membre de l'équipe

Lieu	Intervenant/qualité	Date et heure	Nature de la mission	Durée

Fait à .....Le.....

Nom, prénom du chef de projet
Côté ONMNE avec Signature

Nom, prénom de l'Auditeur avec Signature