**CAHIER DES PRESCRIPTIONS SPECIALES**

APPEL D’OFFRES OUVERT SUR OFFRES DE PRIX

N°03/2019

🙦🙤🙦🙤🙦🙤🙦🙤🙦🙤🙦🙤🙦🙤🙦🙤

OBJET :

AUDIT DE SECURITE DU SYSTEME D’INFORMATION DE L’AGENCE NATIONALE DE REGLEMENTATION DES TELECOMMUNICATIONS

Date limite de réception des plis : le 26/06/2019 à 10h00

PREAMBULE

Le présent appel d’offres ouvert est lancé en application des dispositions de - al. 2, § 1 de l'art. 16 et § 1 de l’art 17 et al. 2, § 3 de l'art. 17 de la décision n°20/2014/DG du 19/12/2014 portant règlement fixant les conditions et les formes de passation des marchés de l’Agence Nationale de Réglementation des Télécommunications.

**Entre :**

L’Agence Nationale de Réglementation des Télécommunications, sise Centre d'Affaires, Boulevard Ar-Ryad, Hay Ryad
BP 2939 - RABAT 10100, représentée par son Directeur Général ou son délégataire, désignée ci-après par « ANRT ».

**D’une part,**

**Et :**

**Le prestataire ou le groupement de prestataires**

**D’autre part,**

Il a été convenu et arrêté ce qui suit :

TITRE I : CAHIER DES PRESCRIPTIONS SPECIALES

CHAPITRE I : DISPOSITIONS GENERALES

**ARTICLE 1 : OBJET DE L’APPEL D’OFFRES**

Le présent appel d’offres ouvert a pour objet l’audit de sécurité du système d’information de l’Agence Nationale de Règlementation des Télécommunications.

**ARTICLE 2 : PIECES CONSTITUTIVES DU MARCHE**

Les pièces constitutives du marché comprennent :

- L’acte d’engagement,

- Le présent CPS,

- Le bordereau des prix – détail estimatif,

- L’offre technique,

- Le CCAG-EMO.

En cas de contradiction ou de différence entre les pièces constitutives du marché, ces pièces prévalent dans l’ordre ou elles sont énumérées ci – dessus.

**ARTICLE 3 : TYPE ET MONTANT DU MARCHE**

Le marché découlant du présent appel d’offres est un marché unique.

Ce marché est réservé à la petite et moyenne entreprise au sens de la Loi 53-00 formant charte de la petite et moyenne entreprise.

Le montant ci-après du marché «**n’est pas à renseigner dans le présent document**» à ce stade**.** Il doit l’être dans l’offre financière et sera transcrit dans cette partie lors de la signature du marché :

|  |  |
| --- | --- |
| **Devise** | En dirhams marocains (MAD) |
| **Montant de la part en MAD hors TVA** | ……………………………………………………*(en lettres et en chiffres)* |
| **Taux de la TVA** | XX (XX) % |
| **Montant de la TVA** | ……………………………………………………*(en lettres et en chiffres)* |
| **Montant avec T.V.A comprise** | ……………………………………………………*(en lettres et en chiffres)* |

**ARTICLE 4 : DOCUMENTS DE REFERENCE**

Pour mener à bien ses missions, l’attention du candidat est portée sur les documents suivants :

* La Loi n°24-96 relative à la Poste et Télécommunications et particulièrement le titre II instituant l’Agence Nationale de Réglementation des Télécommunications promulguée par le Dahir n°1-97-162 du 2 Rabii II 1418 (7 Août 1997) et telle qu’elle a été modifiée et complétée ;
* La Loi n°112-13 relative au nantissement des marchés publics ;
* Le Décret n°2-97-813 du 27 Chaoual 1418 (25 février 1998) portant application des dispositions de la loi n°24-96 relative à la Poste et aux Télécommunications en ce qui concerne l’Agence Nationale de Réglementation des Télécommunications tel qu’il a été modifié et complété ;
* Le Décret n°2-01-2332 approuvant le Cahier des Clauses Administratives Générales applicables aux marchés de services portant sur les prestations d’Etude et de Maîtrise d’œuvre, passés pour le compte de l’Etat ;
* Les Textes législatifs et réglementaires en matière de législation sur les accidents du travail ;
* L’Arrêté du ministre de l’économie et des finances n°20-14 du 8 kaada 1435 (4 septembre 2014) relatif à la dématérialisation des procédures de passation des marchés publics ;
* L’Arrêté du ministre chargé des finances fixant les conditions et les modalités d’application des dispositions relatives à la Petite et Moyenne Entreprise ;
* La Décision n°20/2014/DG du 19/12/2014 portant règlement fixant les conditions et les formes de passation des marchés de l’Agence Nationale de Réglementation des Télécommunications, telle que modifiée et complétée.

Les dispositions de ces textes et documents constituent obligation pour le titulaire. Celui-ci ne pourra en aucun cas se prévaloir de leur ignorance pour s’en soustraire.

**ARTICLE 5 : ENTITE CHARGEE DU SUIVI DE L’EXECUTION**

Pour l’application du marché il y a lieu de préciser que le suivi de l’exécution est assuré par la Division du Système d’Information.

**ARTICLE 6 : ELECTION DE DOMICILE**

Toutes les notifications concernant le marché sont valablement faites à l’adresse précisée dans l’acte d’engagement.

**ARTICLE 7 : VALIDITE DU MARCHE**

Le marché n’est valable, définitif et exécutoire qu’après son approbation par l’autorité compétente**.**

L’approbation du marché doit intervenir avant tout commencement d’exécution des prestations.

**ARTICLE 8 : SOUS TRAITANCE**

Les conditions de sous-traitance sont régies par les dispositions de l’article 141 de la décision n°20/2014/DG précitée.

De ce fait, la sous-traitance est une opération qui intervient dans la phase de l’exécution du marché, c’est-à-dire après que la commission d’appel d’offres ait désigné l’attributaire du marché et après que l’autorité compétente ait notifié à ce dernier l’approbation dudit marché.

Il en découle que la commission d’appel d’offres n’est habilitée à examiner que les capacités juridiques, techniques et financières du concurrent ayant présenté l’offre principale et non pas ses sous-traitants.

Le soumissionnaire doit justifier de ses propres capacités pour la réalisation de cette prestation et non avec celles du ou des sous-traitants.

La sous-traitance n’est pas autorisée dans le cadre du marché issu du présent appel d’offres.

En application du dernier paragraphe de l’article 141 de la décision n°20/2014/DG précitée, les prestations qui ne peuvent faire l’objet de sous-traitance sont constituées par l’ensemble des prestations objets du présent appel d’offres.

**ARTICLE 9 : DROITS D’ENREGISTREMENT**

Le marché doit être enregistré auprès de l’Autorité Administrative Compétente au Maroc. Dans le cas où cet enregistrement est assujetti au paiement de droits, ces derniers sont à la charge et responsabilité totale du titulaire.

**ARTICLE 10 : NATURE ET REVISION DES PRIX**

Les prix sont fermes et non révisables.

Ils sont réputés inclure, pour chaque numéro de prix indiqué dans le bordereau des prix-détails estimatif, tous les frais et sujétions requis pour la réalisation des prestations correspondantes. Le Titulaire ne peut se prévaloir, durant la durée du marché et pour sa réalisation, d’aucune omission ou une mauvaise estimation de la charge de travail, qui relèvent de sa totale responsabilité.

**ARTICLE 11 : REGLEMENT DES SOMMES DUES**

L’ANRT se libérera des sommes dues par elle en faisant donner crédit 60 jours à compter de la date du procès-verbal de réception des prestations et présentation de la facture et de toutes les pièces justificatives exigées. Le paiement s’effectuera par virement au compte bancaire indiqué dans l’acte d’engagement retenu.

La facture doit répondre aux conditions suivantes :

* Etre conforme au bordereau des prix – détail estimatif pour les prestations réalisées ;
* Etre établie en six exemplaires originaux ;
* Etre signée (par la personne habilitée), datée et cachetée ;
* Le montant de la facture doit être arrêté en chiffres et en lettres ;
* Faire ressortir les montants HT, TVA et TTC.

Toute facture ne comportant pas l’identifiant commun de l’Agence Nationale de Réglementation des Télécommunications « ICE n°001696338000043 » sera rejetée par l’Agence et ce conformément aux dispositions de l'article 145-III-4° du Code Général des Impôts et de l’article 8 de la Loi de Finance n°68-17.

Une version électronique de la facture pourra être adressée par courrier électronique à l’ANRT avant édition et transmission de la version papier.

Les factures doivent rappeler les références du marché et l'intitulé exact du compte bancaire du titulaire du marché, l’identifiant commun de l’entreprise ainsi que le RIB composé de 24 chiffres.

**ARTICLE 12 : NANTISSEMENT**

Dans l’éventualité d’une affectation en nantissement du marché, il est précisé que :

* La liquidation des sommes dues en exécution du marché sera opérée par les soins de l’Agence Nationale de Réglementation des Télécommunications.
* Le maître d’ouvrage est chargé de fournir tant au titulaire qu’aux bénéficiaires de nantissement ou subrogations les renseignements et états prévus à l'article 8 de la Loi n°112-13 relative au nantissement des marchés publics.
* Les paiements prévus au marché seront effectués par l’Agent Comptable de l’ANRT, seul qualifié pour recevoir les significations des créanciers du titulaire du marché.

L’ANRT délivrera sans frais au titulaire, sur sa demande et contre récépissé, une copie du marché portant la mention « exemplaire unique » et destiné à former titre pour nantissement conformément à la réglementation en vigueur, et notamment aux dispositions de la Loi n°112-13.

**ARTICLE 13 : PENALITES POUR RETARD**

Conformément au CCAG-EMO, lorsque les délais contractuels sont dépassés, le titulaire encourt sans mise en demeure préalable, une pénalité par jour de retard égale à 5/1000 qui sera retenue d'office sur les sommes dues au titulaire.

Ce taux est applicable au montant du marché augmenté éventuellement des montants des éventuels avenants dans le délai contractuel par jour de retard. Toutefois, le montant total des pénalités qui seront appliquées ne doit pas excéder 10% du montant total du marché.

Lorsque le plafond des pénalités est atteint, l’ANRT est en droit de résilier le marché après mise en demeure préalable et sans préjudice de l’application des autres mesures correctives prévues par le CCAG-EMO.

**ARTICLE 14 : SUIVI DES PRESTATIONS PAR LE TITULAIRE ET EQUIPE PROPOSEE**

Le titulaire devra désigner une équipe, expérimentée et dotée des compétences techniques en relation avec les prestations susmentionnées, qui sera chargée de l’exécution des prestations relatives au marché issu du présent appel d’offres. Le titulaire devra aussi désigner un interlocuteur qui sera responsable de l’exécution du marché issu du présent appel d’offres et du suivi des réalisations avec les responsables désignés de l’ANRT jusqu’à leur validation finale.

Tout changement d’un membre de l’équipe doit être préalablement validé par l’ANRT. Le nouveau membre doit justifier d’un profil et une expérience au moins équivalents à ceux du membre remplacé.

**ARTICLE 15 : CAUTIONNEMENTS**

Par dérogation aux dispositions de l’article 12 du CCAG- EMO, le titulaire est dispensé de constituer le cautionnement provisoire et le cautionnement définitif.

Par dérogation à l’article 40 du CCAG –EMO, il n’est pas prévu de retenue de garantie.

**ARTICLE 16 : RESPECT DE LA CONFIDENTIALITE, SECURITE DES INFORMATIONS ET PROTECTION DES DONNEES PERSONNELLES**

Le titulaire doit s’engager à respecter le principe de confidentialité et ce, par rapport aux informations qui lui seront communiquées éventuellement par l’ANRT et les autres intervenants dans le cadre de cette prestation (Cf. modèle de l’accord de confidentialité en annexe du règlement de la consultation qui sera signé conjointement par le représentant de l’ANRT et par le titulaire et ce, avant le démarrage de l’exécution des prestations objets du présent marché).

Ce dernier devra aussi veiller au respect des dispositions de la loi 09/08 relative à la protection des données personnelles dans le cadre de l’exécution des prestations objets du marché. Ce dernier ne devra en aucun cas conserver ces informations (stockage ou traitement) ou en faire usage pour son propre compte ou pour le compte d’un tiers.

Le titulaire reconnaît que l'exécution des prestations objets du présent marché lui donnera accès à des informations confidentielles de l’ANRT et, que leur divulgation à des tiers aurait des conséquences graves pour l’ANRT. Le titulaire s'engage de ce fait à considérer comme strictement confidentielles toutes les informations de quelque nature qu'elle soit, relatives à l’ANRT, à son système informatique, qu'elle aura recueillies directement ou indirectement à l'occasion du marché. Il en est de même du contenu des fichiers, informations et documents de l’ANRT mis à la disposition du titulaire dans le cadre du présent marché ou saisie au niveau de la plateforme par les utilisateurs de cette Agence.

L’ANRT interdit la consultation de ses documents à toute personne non accréditée par elle.

**ARTICLE 17 : PROPRIETE DES ETUDES**

Tous les documents et rapports établis par le titulaire sont la propriété exclusive de l’ANRT.

**ARTICLE 18 : RESILIATION**

Les conditions de résiliation du marché sont celles prévues par le CCAG-EMO.

**ARTICLE 19 : REGLEMENT DES LITIGES**

A défaut du règlement à l’amiable, les litiges qui se produiraient à l’occasion de l’exécution du marché relèvent de la compétence du tribunal administratif de Rabat.

**ARTICLE 20 : MODALITES DE PAIEMENT**

Le règlement se fera comme suit :

* Pour les phases 1 à 6, le règlement sera effectué à 100% une fois les livrables y afférentes sont achevées et réceptionnées
* Pour la phase 7, le règlement sera effectué à 100% après réception du rapport relatif à chaque mission de ladite phase.

**ARTICLE 21 : DELAI D’EXECUTION**

Le délai d’exécution des phases 1 à 6 est fixé à quatre (4) mois, hors délais de validation et d’arrêts de service.  Ce délai court à partir de la date précisée sur l’ordre de service de commencement. Des arrêts peuvent être prononcés par l’ANRT en cours de réalisation de ces phases.

Le titulaire effectuera l’audit de la plateforme de paiement électronique dans un délai maximal de quatre (4) semaines. Ce délai court à partir de la date précisée sur l’ordre de service de commencement des phases 1 à 6.

La phase 7 fera l’objet d‘un ou plusieurs ordres de services qui lui sont propres correspondant à chaque commande partielle. Le délai d’exécution de chaque commande partielle sera précisé dans cette dernière. Le délai global de cette phase ne peut dépasser 2 ans. Ce délai commence à courir à compter de la date correspondant à la première commande partielle de la phase 7.

**ARTICLE 22 : LIVRABLES**

Les livrables sont les suivants :

1. Rapport de la phase 1 : **Rapport de cadrage de la mission**.
2. Rapport de la phase 2 : **résultats de l’audit environnemental et physique**.
3. Rapport de la phase 3 : **résultats de l’audit**, design d’architecture de sécurité, liste détaillée des vulnérabilités.
4. Rapport de la phase 4 : **résultats des tests d’intrusion**.
5. Rapport de la phase 5 : **rapport d’audit de sécurité applicative**.
6. Rapport de la phase 6 : **rapport de synthèse et rapport détaillé des recommandations et plan d’actions**.
7. Rapports de la phase 7 : **rapport des tests d’intrusion** relatif à chaque commande partielle.

Tous les livrables mentionnés ci-dessus doivent être remis en versions papier et électronique exploitable.

Tous les documents établis dans le cadre du présent audit par le titulaire sont la propriété exclusive de l’ANRT qui pourra les utiliser sans aucune redevance ni restriction.

**ARTICLE 23 : DELAI DE VALIDATION DES LIVRABLES**

- Le délai de validation est fixé à **un (01) mois** après réception du dernier livrable concernant les phases 2 à 6. En cas de dépassement de ce délai, l’ANRT informera le titulaire.

- Le délai de validation est fixé à **quinze (15) jours** après réception du livrable de chaque commande partielle concernant la phase 7. En cas de dépassement de ce délai, l’ANRT informera le titulaire.

La réception doit être matérialisée par un procès-verbal de réception.

Les retards éventuels du fait de l’ANRT ne sont pas imputables au titulaire.

Des ordres d’arrêt motivés et de reprise peuvent être notifiés au titulaire, à tout moment, afin de ne pas comptabiliser dans les délais les retards qui ne lui sont pas imputables.

**ARTICLE 24 : CONDITIONS DE RECEPTION**

La réception sera prononcée à l’issue de la réception des phases 1 à 6.

La réception sera prononcée pour chaque commande partielle de la phase 7.

**ARTICLE 25 : INFORMATIONS**

L’ANRT mettra, dans la mesure du possible, à la disposition du titulaire tout document, information ou donnée jugés nécessaires pour la mission.

Le titulaire doit s’engager à respecter la confidentialité des données et informations dont il aura eu connaissance lors de l’accomplissement de sa mission.

**ARTICLE 26 : ENGAGEMENTS**

* Le titulaire appréciera, sous sa totale responsabilité et charge, l’étendue des tâches à accomplir, compte tenu des objectifs assignés à la présente mission.
* Tous les rapports ainsi que le rapport final appartiendront au Maître d’ouvrage. Le titulaire s’abstiendra de tout usage ultérieur sans l’accord préalable du Maître d’ouvrage.
* Le titulaire garantira la confidentialité des documents mis à sa disposition.
* Les informations et documents jugés utiles pour l’appréciation et la validation des rapports, doivent être communiqués par le titulaire, sous formats papiers et électronique exploitable.
* Le titulaire doit communiquer tout éventuel outil utilisé dans sa mission (fichiers informatiques, …).

**ARTICLE 27 : DROITS DE L’ANRT SUR LES RESULTATS**

L’ANRT dispose de tous les droits sur les résultats des prestations réalisées dans le cadre du présent marché.

CHAPITRE II : DISPOSITIONS PARTICULIERES

**ARTICLE 28 : CONSISTANCE DES PRESTATIONS**

**A- Contexte de la mission**

L’ANRT souhaite réaliser une mission d'audit technique de sécurité de son système d’information. La finalité est de faire une revue globale des composantes du SI (applications métiers, solutions de sécurité, périmétrique et locaux techniques).

**B- Objectifs de la mission**

La présente mission d’audit consiste à mesurer, dans une première étape, le niveau de maturité en matière de sécurité du SI de l’ANRT, et de proposer, dans une deuxième étape, un plan d’actions destiné à consolider les points forts et à proposer les axes d’amélioration ainsi que les actions à entreprendre en vue de mettre en place les bonnes pratiques de sécurité.

Le titulaire assurera la maîtrise d’œuvre de l’audit sur toute sa durée, et établira en collaboration avec l’ANRT :

* Avant le début des missions opérationnelles de l’audit, le calendrier détaillé de réalisation des différentes phases ;
* La liste des tâches intermédiaires et les modalités de leur suivi ;
* Le tableau de bord qui est remis à l’ANRT lors de chaque réunion de suivi d'avancement du projet.

**C- Description du SI ANRT**

Le SI ANRT est constitué des principales solutions applicatives suivantes :

* solution de paiement électronique (PE-ANRT) : l’ANRT a développé une solution de paiement électronique (PE-ANRT) qui utilisera la plateforme de paiement électronique de la TGR (PE-TGR), qui est reliée à celle du CMI. Cette plateforme est composée des principaux éléments suivants :
* des interfaces « Web Services » permettant la communication sécurisée entre la PE-ANRT et la PE-TGR ;
* des interfaces web, accessibles à partir du site web de l’ANRT, mis à la disposition des clients ANRT pour s’identifier et accéder aux factures à régler ;
* la création et la gestion des comptes clients, à partir du site web ANRT ;
* l’accès à une base de données « Facturation » pour y extraire des données et y apporter des maj (via des scripts), à travers le site web de l’ANRT et les « Web Services » cités ci-dessus.
* Services web : notamment les sites web et les applications mobiles accessibles au public.
* Autres solutions développées en interne: facturation & recouvrement, déplacements & congés, traitements de différentes demandes.
* Progiciels : AGIRH, ERPX3, GESTORE, etc.

Ces différentes solutions sont hébergées dans un datacenter interne, comprenant différents serveurs et applications (DNS, WEB, Bases de données, Messagerie, AD, etc.). La plupart des serveurs sont virtualisés.

Des éléments techniques supplémentaires plus détaillés, seront communiqués au titulaire pour cette mission d’audit.

**D- Description des prestations attendues**

Les prestations à fournir dans le cadre du présent appel d’offres sont déclinées en 6 phases.

**Phase 1 : Prise de connaissance**

Cette étape consiste à prendre connaissance du contexte technique, de l’existant en termes d’équipements et d’applicatifs, à définir le plan de travail et préparer le périmètre de l’étude. Il s’agit de prendre connaissance des différentes composantes du SI de l’Agence.

Lors de cette étape, le titulaire devra notamment visiter les locaux de l’ANRT en vue de la réalisation des prospections nécessaires.

Au terme de cette étape, le titulaire doit livrer un ***planning détaillé*** du déroulement de la mission avec les intervenants (CV) de chaque action.

**Phase 2 : Audit environnemental et physique**

Le but de cet audit est d’élaborer les recommandations nécessaires pour fournir une protection environnementale adaptée qui protège les équipements informatiques et les personnes contre les risques humains et naturels.

L’objectif est de cerner la protection du périmètre des équipements informatiques, en terme notamment de :

* Protection du périmètre des ressources informatiques (protection de proximité) et celle des bâtiments (protection des environs) ;
* Politique d’accès au Datacenter ;
* Conformité de l’hébergement aux normes de la sécurité environnementale (sécurités physique et électrique, sécurité incendie, climatisation et humidité, gestion d’accès, etc.).

Le titulaire est tenu de lister les points de contrôle ainsi que les normes et les méthodes qui seront utilisées dans le cadre de cette étape.

Au terme de cette phase, le titulaire doit livrer un rapport comprenant le résultat de l’audit environnemental et physique.

**Phase 3 : Audit de l’architecture et de la configuration**

Cette étape permettra d’examiner le positionnement des différents dispositifs de sécurité mis en place au niveau de l’architecture existante, ainsi que la stratégie de sécurité sur les périmètres internes et externes.

Audit de l’architecture :

Il s’agit de procéder à une analyse très fine de l’infrastructure réseau touchant le paramétrage et la configuration des équipements et logiciels de filtrage et de détection, ainsi que les hôtes et les équipements d’interconnexion pour s’assurer du respect des bonnes pratiques et des recommandations en matière de sécurité quant à l’emplacement des actifs réseaux et sécurité, le cloisonnement, l’échange des flux, les réseaux sans fil, etc.

Audit de configuration :

Le but de cet audit de configuration est d’examiner la complétude des fichiers de configuration et de vérifier leurs conformités par rapport aux meilleures pratiques dans le domaine, et ce afin d’identifier les faiblesses éventuelles et de proposer un paramétrage permettant de combler ces faiblesses. D’autre part, le titulaire doit réaliser les analyses et revues des configurations pour les éléments suivants :

* Pour le réseau : équipements actifs et passifs (pare-feu, routeurs, …), architecture logique, plan d’adressage, détection automatique de vulnérabilités, liens télécoms, etc.
* Pour les serveurs et les applications : dispositifs de sécurité (antivirus, IPS), authentification, dispositifs de supervision et de détection des cyberattaques, cryptographie, mises à jour et patch, systèmes d’exploitation, services réseau et Internet, ports d’accès aux services, messagerie, bases de données, dispositifs de journalisation et d’analyse des journaux, accès à distance, gestion des profils et privilèges, gestion des formats de données, etc.

Au terme de cette phase, le titulaire doit livrer un rapport comprenant notamment :

* Les procédures de gestion à mettre en place ;
* Un design d’architecture de sécurité élaboré en tenant compte des failles de sécurité identifiées, du dimensionnement du réseau ainsi que des nouvelles menaces auxquelles il faudrait faire face ;
* La liste détaillée des vulnérabilités, classifiées en fonction de leur gravité potentielle (conséquences, facilité d’exploitation, …).

Le périmètre siège inclut :

* Echantillon de 10 serveurs ;
* Echantillon de 3 switchs ;
* Echantillon de 2 routeurs ;
* Echantillon de 5 postes de travail ;
* Echantillon de 3 équipements de sécurité.

Le périmètre du site distant (une vingtaine d’utilisateurs qui accèdent au réseau local de l’ANRT siège) :

* Echantillon d’un switch ;
* Echantillon d’un routeur ;
* Echantillon d’un poste de travail.

**Phase 4 : Tests d’intrusion dans le cadre de l’audit initial**

Il s’agit de mener des opérations de simulation d’attaques, d’intrusions internes et externes, de cracking (craquage) de mots de passe, de piratage, de vols d’informations, de fraude, d’accès illicites ou malintentionnés, et de toute autre forme d’attaque envisageable. Ceci dans l’objectif d’apprécier la robustesse du SI de l’ANRT et sa capacité à préserver l’intégrité de ses données.

Ces tests doivent être menés selon une méthodologie à détailler par le titulaire et en utilisant les outils nécessaires et conformément à l’éthique et les règles d’art en la matière. Cette méthodologie doit être préalablement validée par l’ANRT.

Les tests intrusifs, qui doivent être menés en dehors des horaires de trafic important, ne doivent en aucun cas altérer, modifier ou détruire les données du SI de l’ANRT, ni perturber le bon fonctionnement de ce dernier. Il sera de la responsabilité du titulaire de mettre en garde, prévenir et conseiller l’ANRT de tous les risques encourus lors de la mise en œuvre de ces tests.

Pour les tests d’intrusion externes, ils se dérouleront comme suit :

* Etape N°1 (en boite noire) : Les experts du titulaire procéderont à ces tests en disposant uniquement des informations publiques. Cette phase de découverte a pour objectif :
* D’obtenir un maximum d’informations sensibles sur les services accessibles et les équipements d’infrastructure associés, en cartographiant la plate-forme internet grâce à différentes techniques ;
* D’identifier des vulnérabilités présentes sur les machines exposant les services cartographiés ;
* D’énumérer les exploitations possibles de vulnérabilités trouvées et d’évaluer les risques d’intrusion dans les systèmes de l’ANRT.
* Etape N°2 (en boite blanche) : Plus de détails seront communiqués sur la configuration au titulaire, pour effectuer ce test d’intrusion. L’auditeur devra évaluer la robustesse des mécanismes d’authentification (principes et algorithmes utilisés), de gestion de session, de cloisonnement des données, de contrôle des paramètres transmis par l’utilisateur. Il est important de s’assurer qu’un utilisateur standard ne peut élever ses privilèges sans autorisation, afin d’obtenir des informations confidentielles ou d’insérer des données falsifiées.

Au terme de cette phase, le titulaire doit livrer un rapport comprenant le ***résultat des tests d’intrusion*** (internes et externes) avec une indication précise de l’impact des vulnérabilités recensées sur la sécurité, la confidentialité, l’intégrité et la disponibilité du SI et la manière de les combler. Ce rapport devra comprendre notamment :

* La description du risque potentiel ;
* Les conséquences potentielles ;
* Le coût de réparation des dommages ;
* La probabilité de la réalisation du risque ;
* La description des actions préventives.

Pour la partie web, le titulaire doit effectuer toutes les évaluations nécessaires pour assurer la non-existence de vulnérabilités potentielles qui peuvent constituer un impact sur le SI de l’ANRT. Il doit par la suite présenter un rapport de niveau de maturité des services web de l’ANRT avec la liste des vulnérabilités de la dernière version actuelle de l’OWASP.

**N.B : Il convient de préciser que, pour les phases 2 à 4, le titulaire doit informer immédiatement l’ANRT des constats et des premières conclusions lorsqu’il s’agit de vulnérabilités majeures et critiques qui nécessiteraient une action rapide.**

**Phase 5 : Audit de sécurité applicative**

Cette étape consiste à tester le niveau de sécurité des applications afin d’identifier et d’évaluer les vulnérabilités existantes. L’identification des failles se fera sur la base de la dernière version des Top 10 de l’OWASP.

Cette étape porte également sur l’évaluation de la sécurité des mécanismes de contrôle d’accès et des habilitations et doit permettre de vérifier l’application des politiques et bonnes pratiques au niveau de l’application et surtout le contrôle d’accès et le cloisonnement des profils.

Dans tous les cas, les tests visant à réaliser un déni de service seront proscrits par défaut, mais pourront être envisagés de manière exceptionnelle et sur autorisation explicite de l’ANRT, en cas d’une forte suspicion de la part du titulaire quant à l’existence d’une vulnérabilité de cette nature.

Périmètre : 10 applications WEB.

**Phase 6 : Élaboration des recommandations et d’un plan d’actions**

A l’issue de ses travaux, le titulaire s’engage à mettre à la disposition de l’ANRT un rapport d’audit comprenant 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.

Ces recommandations doivent être réalistes, pragmatiques et hiérarchisées en fonction de l’importance des risques détectés.

Le titulaire devra mettre en œuvre un plan d’actions qui permettra à l’ANRT d’implémenter les recommandations de sécurité et de suivre leur application. Ce plan d’actions doit faire partie du rapport d’audit précité.

Le rapport d’audit doit rester confidentiel et ne doit être communiqué qu’à l’ANRT.

Aussi, une réunion de clôture de l’audit doit être tenue par le titulaire pour présenter le rapport d’audit.

Au terme de cette phase, le titulaire doit livrer le rapport d’audit qui comprend :

* Un état des recommandations pour la mise à niveau de l’existant ;
* Le plan d’actions de mise en conformité.

**Phase 7 : Tests d’intrusion à la demande**

Il s’agit de mener des tests d’intrusion, à la demande de l’ANRT, et ce selon les mêmes modalités et exigences de la phase 4 ci-dessus. Cette prestation fera l’objet de commandes partielles, dont chacune précisera la durée allouée aux tests d’intrusion.

Pour chaque intervention relative à une commande partielle, le titulaire devra fournir :

* La liste des intervenants et leurs CV à approuver par l’ANRT ;
* Un plan de charge détaillé ;
* Un planning de réalisation détaillé ;
* La liste des prérequis attendus de l’ANRT.

**E- Exigences de confidentialité**

Le titulaire aura accès à des informations sensibles liées au fonctionnement et à la sécurité du SI de l’ANRT, il est alors tenu de :

* Présenter son engagement de confidentialité à l’ANRT, conformément au modèle qui lui sera communiqué par l’ANRT ;
* Ne communiquer aucune information concernant cette mission au public ni à une tierce partie sans le consentement écrit de l’ANRT ;
* Garantir que le circuit de production des documents liés à la présente mission d’audit est sécurisé (poste de travail, circuit de validation interne, impression des documents, sauvegarde des documents, destruction des documents, etc.) ;
* Avoir une politique de diffusion de documents selon leur niveau de confidentialité. Tous les documents résultant de l’audit doivent avoir une diffusion restreinte aux personnes concernées par l’audit ;
* Mettre en place un système sécurisé pour le partage des rapports et livrables avec l’ANRT.

**F- Conformité aux normes et réglementations en vigueur**

Cette mission d’audit doit être effectuée dans le respect des lois et normes en vigueur, notamment :

* La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;
* La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données.
* La directive Nationale de la sécurité des systèmes d’information (DNSSI) élaborée par la Direction Générale de la Sécurité des Systèmes d’Information (DGSSI).

# TITRE II :

**Bordereau des prix-détail estimatif**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N° DES PRIX****1** | **Désignations des prestations****2**  | **Unité de mesure ou de compte****3** | **Quantité****4** | **Prix unitaire en DH****Hors TVA En chiffre****5** | **Prix Total en DH Hors TVA****6 = 4 x 5** |
| **01** | Audit de sécurité du SI ANRT (phases 1 à 6) | Forfait |  |  |
| **02** | Tests d’intrusion à la demande (phase 7)  | Jour/ Homme | 30 |  |  |
| **Montant hors T.V.A. en dirhams**  |  |
| **Taux de la T.V.A.**  |  |
| **Montant de la T.V.A. en dirhams**  |  |
| **Montant T.V.A. comprise en dirhams** |  |

 **Signatures[[1]](#endnote-1)** A: …………….., le ……………………..

 **Signature et cachet du Concurrent**

1. Lors de la signature du marché, le Maître d’Ouvrage signe ce **Bordereau des prix-détail estimatif**  [↑](#endnote-ref-1)