

COMPAGNIE TUNISIENNE DE FORAGE

19 RUE DE L'ARTISANAT - 2080 ARIANA - CHARGUIA II-TUNISIE
FAX N° (216-70) 836 568 – 837 041 PHONE N° (216-70)837 322

OBJET : CONSULTATION N° **PP26/548**

Mission d'audit réglementaire de la sécurité du système d'information

La Compagnie Tunisienne de Forage (C.T.F.) souhaite mandater un bureau d'études pour réaliser une mission d'audit réglementaire de la sécurité du système d'information (SSI), conformément aux exigences précisées dans l'annexe I ci-joint.

A cet effet, nous vous invitons à nous soumettre votre meilleure offre de prix en **TTC** conformément à la procédure ci-dessous.

PROCEDURE DE SOUMISSION :

Les offres doivent parvenir à la CTF :

Par plis fermés :

A l'adresse suivante 19 rue de l'Artisanat charguia 2 -2035 L'Aéroport Tunis-Tunisie, par voie postale sous plis scellés et recommandés ou par rapid poste, ou déposé au bureau d'ordre de CTF contre décharge.

L'enveloppe doit :

* être adressée au nom de :

Monsieur le Président Directeur Général

* Porter uniquement :

- L'adresse de la CTF,
- Les références de la consultation (PP 26/548)

- La mention " NE PAS OUVRIR "

* contenir à l'exclusion de tout autre document :

-Les documents demandés au niveau de cahier de charge

Le texte de la consultation & les annexes, dûment signés et portant obligatoirement le cachet du soumissionnaire.

- Le bordereau de prix en ANNEXE 11 dûment rempli, signé et portant obligatoirement le cachet du soumissionnaire.

- Document justificative relative à la référence proposée

-Les offres doivent parvenir dans les meilleurs délais mais pas plus tard que le

26.10.2026 à 17H

Toute offre parvenue après les délais sera rejetée (le cachet du Bureau D'ordre de la CTF faisant foi pour les).

Méthodologie d'évaluation

Les offres financières, après la correction des éventuelles faute de calcul, seront classées du moins disant au plus disant sur la base du montant total et sera retenue l'offre moins disante qui sera conforme techniquement aux prescriptions de la présente consultation.

Conditions particulières

- Les offres reçues dans les délais doivent rester valables au moins 120 jours et ce à compter du lendemain de la date limite de réception des offres.
- Le mode de paiement est de 45 jours, par virement bancaire, date réception de votre facture.

SALUTATIONS

C.T.F.

P/DIRECTION APPROVISIONNEMENT & MARKETING



ANNEXE I

Clauses Techniques

Audit réglementaire de la sécurité du Système d'Information

Compagnie Tunisienne de Forage (CTF)

Référence : PP26-548

Date : 30/09/2026



Article 1 : OBJET

La mission objet de cet appel d'offres concerne l'audit de la sécurité du système d'information au niveau des structures décrites dans l'annexe 7.

Cet audit devra se conformer, au minimum, aux dispositions énoncées dans le décret-loi 2023-17 du 11 mars 2023 et organisé par 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, 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, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité de l'information.

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.

Article 2 : CONDUITE ET DEROULEMENT 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, 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 :

Une session de sensibilisation préliminaire, destinée au comité et à la cellule de sécurité du système d'information, devra être proposée.

Cette session préliminaire aura pour premier objectif une sensibilisation générale aux dangers cybernétiques et aux risques cachés encourus, incluant notamment la présentation pratique d'attaques cybernétiques. Elle devra également rappeler les objectifs de l'audit, son urgence et les bienfaits attendus, ainsi que garantir la confidentialité des données reçues.

A la fin de cette opération un PV sera dressé et signé conjointement par le titulaire et le maître 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 d'une session 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 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 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, ...).

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 chômage.

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 sagement 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, switches, ...),



- 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,).

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 audité.

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 classer 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 maître 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 8 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 : METHODOLOGIE(S) ADOPTEE(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

- 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 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.

Article 4 : LIVRABLES

Le titulaire du marché doit remettre tous les livrables tels que détaillés dans l'annexe 5 et affinés lors de la phase de cadrage de la mission.

Le titulaire doit remettre notamment :

- 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.

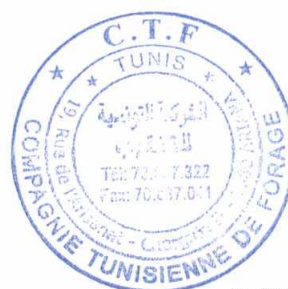
Les livrables sont à fournir en langue française, en format papier et en format numérique exploitable (Word, Excel, PowerPoint)

Tous les livrables sont la propriété exclusive de la Compagnie Tunisienne de Forage.

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



Annexes



ANNEXE 1 :

Tableau de conformité technique

Conditions	Minimales exigées	Justificatifs	Réponse du soumissionnaire	Valeur minimale	Points Bonus-attribués = Valeur réponse du soumissionnaire – Valeur Minimale
SOUSSIONNAIRE					
Le soumissionnaire est habilité par l'Agence Nationale de la Cyber Sécurité, conformément aux exigences réglementaires du Décret-loi n° 2023-17 du 11 mars 2023, relatif à la cybersécurité, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité de l'information.	oui	Certifié par l'ANCS en cours de validité		oui	
Références minimales en Tunisie dans une mission d'audit réglementaire de sécurité SI	Au moins 05 références pendant les 5 dernières années. (2020)	Attestations de bonne fin de mission fournie par le client		05	
Références minimales dans des organismes de taille équivalente à la CTF (multisite avec un effectif supérieur à 140) en Tunisie, dans une mission d'audit réglementaire de sécurité SI	Au moins 03 référence pendant les 5 dernières années. (2020)	Attestations de bonne fin de mission fournie par le client		03	
ÉQUIPE DU PROJET					
L'équipe chargée de la mission doit comporter au minimum les profils suivants : - Un Chef de Projet - deux membres sénior - Un membre experts techniques -Le nombre d'intervenants supérieur à 3 n'engendre pas de points bonus complémentaires					
Qualifications minimales du Chef de projet	-(01) membre Permanent	Oui (CNSS, etc.)		Oui	
	-Au minimum Bac+5	Diplôme Bac +5		Oui	
	Expérience dans le domaine Sécurité SI : 10 ans	CV et justificatifs		10	
	Avoir au moins 03 références en Tunisie en tant que chef de projet dans des missions d'audit réglementaire de sécurité SI	Attestations de bonne fin de mission fournie par le client		03	
	-Dispose d'un certificat LEAD AUDITOR en cours de validité à la date limite des remises des offres	Certificats en cours de validité à la date limite de remise des offres		01	
Qualifications minimales des membres sénior	-membre Permanent	Oui (CNSS, etc.)		Oui	
	Au minimum Bac+5	Diplôme Bac +5		Oui	

	-5 ans d'expérience	CV et justificatifs		05	
	-Au moins 02 référence en Tunisie dans des missions d'audit réglementaire de sécurité SI	Attestations de bonne fin de mission fournie par le client		02	
	-Dispose d'un certificat ITIL et/ ou LEAD AUDITOR et/ou ISO 27001 et/ou ISO 22301 et/ou ISO 27032 et	Certificats en cours de validité à la date limite de remise des offres		01	
Qualification minimale du membre expert technique	-membre <u>Permanent</u>	Oui (CNSS, etc.)		Oui	
	Au minimum Bac+5	Diplôme Bac +5		Oui	
	03 ans d'expérience au minimum	CV et justificatifs		03	
	-Au moins 02 référence en Tunisie dans des missions d'audit réglementaire de sécurité SI	Attestations de bonne fin de mission fournie par le client		02	
Services					
Conduite de la mission	Présentation de la méthodologie de conduite du projet conformément aux exigences citées en : Article 2.			Oui	
Livrables	Le titulaire du marché doit remettre tous les livrables tels que détaillés dans l'Annexe 5			Oui	
Délais d'exécution hors délai de validation par la Compagnie Tunisienne de Forage et levée des réserves	90 jours			Oui	

NB : Les critères mentionnés dans les trois tableaux ci-dessus doivent être obligatoirement justifiés par les pièces (diplômes, certifications, attestations du client, PV de réception, CNSS).

Fournir une seule page pour chaque pièce ou justificatif exigé,

Les références doivent être signées par l'organisme émetteur, spécifier la nature de la mission et spécifier les contacts utiles.

La réponse du soumissionnaire sera éventuellement corrigée par les pièces justificatives fournies.

Date, Signature et cachet

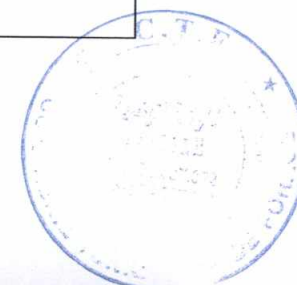


ANNEXE 2 :

global de la mission

Planning Global d'Exécution de la mission (Hors délais de validation par la Compagnie Tunisienne de Forage) :

Composant		Equipe intervenante	Durée de la mission (en Homme/jour)	Livrable
Phase	Objet de la sous phase			
Volet d’audit organisationnel et physique	1. ...			
	2. ...			
	3. ...			
	4. ...			
Volet d’audit technique	1. ...			
	2. ...			
	3. ...			
	4. ...			
Volet d’appréciation des risques	1. ...			
	2. ...			
	3. ...			
	4. ...			
Volet Sensibilisation	1. ...			
	2. ...			
	3. ...			
	4. ...			
Signature et cachet du soumissionnaire				
Noms et signatures de(s) auditeur(s) certifié(s)				



ANNEXE 3

Structure du capital de la société soumissionnaire

Raison sociale :

N° de Matricule Fiscal :

Inscrit au registre de commerce sous le numéro :

Adhérent à la CNSS sous le n°

Adresse :
.....
.....

Téléphone : Fax :

Statut de la société : Sarl : S.A. :

Capital : DT

Activités de la société :
.....
.....
.....

Personnel de la société :

- Nombre de(s) ingénieur(s)
- Nombre d'auditeurs en Informatique (Sécurité, Système d'information, tc.)
- Nombre des techniciens.....
- Total du personnel.....

Nom de la Personne bénéficiant de la procuration et signant les documents relatifs à l'offre
.....

Qualité de cette personne (fonction)

Tunis le,

Lu et approuvé

Signature et cachet du soumissionnaire



ANNEXE 4

Accord de non divulgation

ACCORD DE NON-DIVULGATION

Objet

Le présent Accord de Non-Divulgence (ci-après « l'Accord ») a pour objet de définir les conditions dans lesquelles le Prestataire, dans le cadre de la mission d'audit réglementaire du Système d'Information de la Compagnie Tunisienne de Forage (CTF), s'engage à préserver la confidentialité des informations auxquelles il aura accès.

Définition des Informations Confidentielles

Sont considérées comme Informations Confidentielles, sans que cette liste soit limitative, toutes les informations communiquées sous forme écrite, orale, électronique ou autre, notamment :

- Informations techniques, organisationnelles, opérationnelles et stratégiques
- Architecture du système d'information, configurations, schémas réseau
- Comptes, identifiants, journaux, rapports, résultats de tests et d'audit
- Données personnelles, données sensibles ou critiques
- Documents internes, procédures, politiques de sécurité (PSSI, PCA, PRA, etc.)
- Informations relatives aux locaux, sites, dispositifs de sécurité physique
- Informations concernant les partenaires, prestataires ou sous-traitants de la CTF

Obligations du Prestataire

Le Prestataire s'engage à :

- Utiliser les Informations Confidentielles exclusivement dans le cadre de la mission d'audit définie par le cahier des charges.
- Ne pas divulguer, transmettre ou rendre accessibles les Informations Confidentielles à des tiers non autorisés.
- Mettre en œuvre toutes les mesures nécessaires pour assurer la protection des Informations Confidentielles.
- Limiter l'accès aux Informations Confidentielles aux seules personnes strictement nécessaires à la mission.
- Ne pas copier, reproduire ou conserver les Informations Confidentielles au-delà de ce qui est requis pour la mission.

Exceptions

Les obligations de confidentialité ne s'appliquent pas aux informations qui :

- Sont ou deviennent publiques sans violation du présent Accord
- Doivent être divulguées en vertu d'une obligation légale ou réglementaire, sous réserve d'en informer préalablement la CTF

Restitution des informations

À l'issue de la mission ou sur demande de la CTF, le Prestataire s'engage à :



- Restituer l'ensemble des documents et supports contenant des Informations Confidentielles
- Détruire toute copie, sous quelque forme que ce soit, et en fournir attestation sur demande

Responsabilité

Toute violation du présent Accord engage la responsabilité du Prestataire, sans préjudice des dommages et intérêts que la CTF pourrait réclamer conformément à la législation en vigueur.

Droit applicable et juridiction compétente

Le présent Accord est régi par le droit tunisien.

Tout litige relatif à son interprétation ou à son exécution relèvera de la compétence des juridictions tunisiennes compétentes.

Entrée en vigueur

Le présent Accord entre en vigueur à la date de sa signature.

Fait à :

Le :

Signature et cachet du soumissionnaire

ANNEXE 5

Répartition des exigences minimales des livrables par phase ⁽¹⁾:

Phase	Précision	Démarche	Livrable
Phase 1 Déclenchement de l'audit	Planification	Lancement Cadrage Périmètre	Présentation de lancement Planning PV de lancement
Phase 2 Sessions de sensibilisation Pré-audit Revue des documents	Une session de sensibilisation d'une demi-journée pour un groupe de 20 personnes, dans les locaux de la société. Analyse documentaire.	Préparation du support de sensibilisation Déroulement des sessions Analyse des écarts	Support de sensibilisation Analyse des écarts
Phase 3 Audit organisationnel et physique	Conformément aux exigences réglementaires et aux bonnes pratiques ISO/IEC 27001.	Analyse documentaire Entretiens Visite des locaux Elaboration du rapport	Rapport d'Audit Organisationnel et physique
Phase 3 Tests d'intrusion externes	Toutes adresses IP publiques	Lancement des tests d'intrusion externes Elaboration du rapport	Rapport de Tests d'intrusion externes
Phase 3 Tests de phishing et social engineering	Au moins 02 scénarii de phishing	Préparation des scénarii de phishing/social engineering Lancement des scénarii de phishing/social engineering Elaboration du rapport	Rapport de Tests de phishing/social engineering
Phase 3 Tests d'intrusion internes	type de scénarii à simuler : - Invités - Utilisateurs - Informaticiens	Lancement des tests d'intrusion internes Elaboration du rapport	Rapport de Tests d'intrusion internes
Phase 3 Audit de l'infrastructure réseau et sécurité	à affiner lors de la phase de cadrage	Audit de l'architecture réseau et des pratiques de gestion Audit de configuration Elaboration du rapport	Rapport d'Audit de l'infrastructure réseau et sécurité
Phase 3 Audit de la sécurité de l'infrastructure système	à affiner lors de la phase de cadrage	Audit de l'architecture système et des pratiques de gestion Audit de configuration Elaboration du rapport	Rapport d'Audit de la sécurité de l'infrastructure système
Phase 3 Audit de la sécurité de l'infrastructure applicative	Au moins 2 applications à affiner lors de la phase de cadrage.	Tests d'intrusion applicatifs. Audit de l'architecture applicative et des pratiques de gestion. Audit de configuration.	Rapport d'Audit de la sécurité de l'infrastructure applicative

Phase	Précision	Démarche	Livrable
Phase 4 Elaboration du rapport d'Audit sous le format de l'ANCS	Conformément aux termes de référence exigés par l'ANCS	Analyse des risques Consolidation des résultats d'audit Préparation du plan d'actions organisationnelles et physiques Préparation du plan d'actions techniques	Rapport d'Audit de la Sécurité du Système d'Information
Phase 5 Sessions de sensibilisation Post-audit	7 sessions de sensibilisation d'une demi-journée chacune, pour 7 groupes de 20 personnes, dans les locaux de la société	Préparation du support de sensibilisation Post-audit Déroulement des sessions	Support de sensibilisation Post-audit
Clôture de l'audit	Une session de présentation pour le top management de la société		Rapport de synthèse des résultats d'audit PV de clôture

(1)

- Le soumissionnaire peut proposer toute amélioration jugée utile concernant le découpage en prestations du projet et la consistance de chaque prestation. Toutefois toutes les prestations demandées doivent être incluses dans sa proposition.
- Le soumissionnaire doit mettre à la disposition de La Compagnie Tunisienne de Forage tous les livrables cités, ainsi que les livrables estimés par la société ou par lui-même nécessaires à la mission
- Le détail des phases est décrit dans l'**article 2 « Conduite et déroulement de la mission »** du cahier des clauses techniques particulières.

Fait à, le.....

Cachet & Signature du Soumissionnaire



ANNEXE 6

Méthodologie de conduite de 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'audit, 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 :

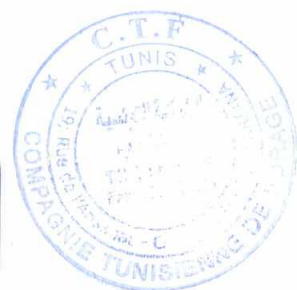
- Méthodologie d'Audit technique, incluant le type et l'objet des tests* à réaliser pour chaque phase de l'audit technique suivant:
 - Audit de l'architecture
 - Audit de la configuration de chaque type de composantes du périmètre de l'audit présentées dans l'annexe 7 (Description volumétrique des structures à auditer)
 - Audit intrusif.
- Outils utilisés pour réaliser les tests pour chacune des phases de l'audit technique suscitées,
- 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.

Fait à, le.....
Cachet & Signature du Soumissionnaire



ANNEXE 7

Description du système d'Information actuel

Le système d'informations actuel de La Compagnie Tunisienne de Forage (à vous communiquer au cours de la mission)

1. ORGANISATION SOMMAIRE DE LA COMPAGNIE TUNISIENNE DE FORAGE

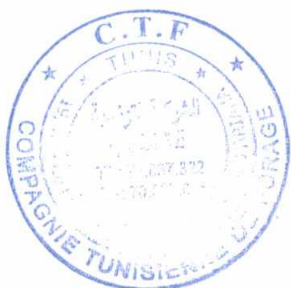
La Compagnie Tunisienne de Forage est organisée de la manière suivante :

- **Le niveau Central** : il s'agit du siège social sis à Charguia II, Ariana. ;
- **Cloud Externe** : Tunis
- **Le niveau distant** : actuellement, on compte 8 sites distants
 - Base logistique de Sfax : sis à la zone industrielle de Sidi Salah
 - Rigs (chantiers de forage). ;

L'effectif de La Compagnie Tunisienne de Forage est aux alentours de 425 employés,

2. STRUCTURES DE LA COMPAGNIE TUNISIENNE DE FORAGE A AUDITER SUR LES LIEUX

		Lieu d'implantation (gouvernorat)	Nombre de micro-ordinateurs	Nombre de serveurs	Nombre de Switchs / Routeurs	Nombre d'applications / BD
1	Siège social	Ariana, Charguia II	80	14 physiques 11 virtuelles	10 Switchs 1 Routeur	6 SQL
2	Cloud Externe	(À auditer à distance)	0	4 virtuelles	0	3 Oracle
3	Base logistique	Sfax	40	1 physique 1 virtuelle	3 Switchs 1 Routeur	0
4	Rig OX	(À auditer à distance) À vous communiquer au cours de la mission	30	0	0 Switch 1 Routeur/site	0



ANNEXE 8 :

La liste des références du soumissionnaire

Référence	Nature	Date début de la mission	Date fin de la mission	Observations

Chaque référence doit être justifiée par les PVs de réception ou des attestations de bonne fin de mission.

Fait à, le.....

Cachet & Signature du Soumissionnaire



ANNEXE 9 :
La liste des intervenants

Nom & Prénom	Profil : (chef de projet / Sénior / expert technique)	Diplôme	Certificats	Références

Les diplômes des intervenants, leurs certificats fournis de la part d'un organisme de certification ainsi que les justificatifs de leurs références

Fait à, le.....

Cachet & Signature du Soumissionnaire



ANNEXE 10 :

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 11 :

Bordereau des prix :

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

Soumissionnaire :

Code d'identifiant fiscal :

Rubriques	Montant Hors Taxes	Taux TVA	Montant TVA	Montant TTC
Audit Organisationnel et physique Prix forfaitaire HT en toutes lettres :				
Audit Technique Prix forfaitaire HT en toutes lettres				
Analyse et évaluation des risques Prix forfaitaire HT en toutes lettres				
Sessions de sensibilisation Prix forfaitaire HT en toutes lettres				
Prix total Prix HT en toutes lettres				

Fait à, le.....
Cachet & Signature du Soumissionnaire

