

# **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° PP25/660**

**Mission d'audit externe application Open PGI**

*La Compagnie Tunisienne de Forage (C.T.F.) souhaite mandater un bureau d'études pour réaliser une mission d'audit et de revue des accès utilisateurs à ses systèmes critiques, notamment ceux liés aux opérations comptables et financières, à la distribution et à la gestion des données sensibles, conformément aux exigences précisées dans l'annexe 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.*

### **A/L'enveloppe externe doit :**

*\* être adressée au nom de :*

*Monsieur le Président Directeur Général*

*\* Porter uniquement :*

- *L'adresse de la CTF,*
- *Les références de la consultation (PP 25/660)*
- *La mention " NE PAS OUVRIR"*
- *(Ni le nom, ni le sigle ni aucune autre indication pouvant renseigner sur l'identité du soumissionnaire ne doivent figurer sur cette enveloppe).*

*\* Contenir :*

*Une autre enveloppe interne cachetée*

### **B/L'enveloppe interne doit :**

*\* porter :*

- *la mention " : OFFRE TECHNIQUE ET FINANCIERE"*
- *le nom et l'adresse du soumissionnaire*

*\* 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 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 **19 Janvier 2026 à 17h.** Toute offre parvenue après les délais sera rejetée (le cachet du Bureau D'ordre de la CTF faisant foi pour les plis et la date & l'heure pour les mails).*

**Méthodologie d'évaluation :**

*Les offres financières, après la correction des éventuelles faute de calcul, seront classées du moins disant au plus disant, 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 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.

DIRECTION APPROVISIONNEMENT & MARKETING

## **ANNEXE**

**Mission d’Audit et de Revue des Accès Utilisateurs aux  
Systèmes d’Information**

**Entreprise : Compagnie Tunisienne de Forage (CTF)**

**Date : 06-01-2026**

## 1. Contexte

Dans le cadre du renforcement de la gouvernance des systèmes d'information, la Compagnie tunisienne de Forage CTF souhaite mandater un bureau d'Etudes pour mener une mission d'audit et de revue des accès utilisateurs à ses systèmes critiques, notamment ceux liés aux opérations comptables et financières, de distribution et de gestion des données sensibles.

La gestion des identités et des accès (IAM - Identité and Access Management) est un enjeu majeur pour la protection des actifs informationnels, la conformité aux exigences réglementaires (ISO 27001, ANCS, etc.) et la réduction des risques opérationnels et de cyber sécurité.

## 2. Objectifs de la mission

L'objectif principal de la mission est de :

- Vérifier l'efficacité du dispositif actuel de gestion des identités et des accès (IAM).
- Identifier les anomalies : comptes orphelins, partagés, inactifs, super-utilisateurs non contrôlés (droits d'accès excessifs, inappropriés ou obsolètes).
- Une **analyse de la traçabilité des interventions** (qui a fait quoi, quand, et sur quoi).
- Déetecter les connexions suspectes (hors horaires ouvrés, week-ends, échecs répétés).
- Évaluer l'efficacité des contrôles de sécurité existants sur l'application et sa base de données et la conformité avec les normes ISO 27001:2022 et le Décret-loi [écret-loi 2023-17 du 11 mars 2023](#).
- Proposer un **plan d'actions correctives** priorisé.

## 3. Portée de la mission

La mission couvrira les aspects suivants : revue des opérations et des attributions d'accès aux systèmes suivants : Open PGI et sa base de données Oracle afin de pouvoir faire une analyse complète des logs et les rapprocher avec les profils d'utilisateurs et pour identifier éventuellement toute incohérence ou risque inhérent de la configuration historique/existante des droits d'accès.

### a. Périmètre fonctionnel

- Application OPENPGI, incluant les modules **Open PRH** et **Open Finance**.
- Profils utilisateurs concernés :
  - Internes (employés),
  - Externes (prestataires),
  - Temporaires ou comptes techniques.

### b. Périmètre technique

- Application OPENPGI et sa base de données Oracle (toutes les couches applicatives et de stockage concernées).
- Gestion des accès : contrôle des habilitations, des priviléges administratifs et techniques, et du respect du principe du moindre privilège.
- Analyse des journaux de sécurité (logs) et des événements applicatifs et systèmes.
- Analyse de la traçabilité des interventions :
  - Identification de **qui** a réalisé chaque action,
  - **Quand** elle a eu lieu,
  - **Sur quels éléments** (modules, tables, paramètres, comptes, etc.),
  - Et **dans quel contexte** (opération planifiée, correctif, maintenance, ou action non autorisée).

### c. Périmètre géographique

- Sites concernés : siège social.

### d. Période auditée

- Accès en vigueur sur les 12 mois de l'année 2024, avec un focus sur les mouvements de personnel (entrées, sorties, mutations).

## 4. Méthodologie

La mission d'audit comprendra :

1. **Collecte documentaire** : politiques IAM, procédures, journaux de connexion et de modification (logs applicatifs et base de données).
2. **Entretiens** : RSSI, DI, RH, responsables métiers, et administrateurs techniques.
3. **Analyse technique** : extraction et revue des droits d'accès, rapprochement avec rôles et responsabilités.
4. Analyse technique :
  - Extraction et revue détaillée des droits d'accès utilisateurs et administrateurs.
  - Rapprochement entre les privilèges attribués et les responsabilités réelles.
  - **Analyse approfondie des interventions et modifications** réalisées sur l'application et sa base de données :
    - Identification de **qui** a effectué chaque opération,
    - **Quand** et **sur quels objets** (tables, modules, comptes, paramètres),
    - Vérification de la **conformité des interventions** avec les habilitations officielles.
5. **Tests de conformité** : échantillonnage d'utilisateurs, vérification du principe du moindre privilège et du respect des procédures de validation.
6. **Évaluation des risques** : cartographie des écarts, hiérarchisation selon l'impact et la probabilité, formulation de recommandations correctives.

## 5. Résultats attendus

Le rapport d'audit devra inclure :

- Un **état des lieux détaillé** des accès par système, rôle et profil utilisateur.
- L'**identification des anomalies** : accès non justifiés, comptes orphelins, super-utilisateurs non contrôlés, priviléges excessifs, etc.
- Une **analyse complète de la traçabilité des interventions**, précisant :
  - Les actions effectuées,
  - Les comptes utilisés (notamment *master* ou équivalents),
  - Les modules et données impactés,
  - Les éventuelles irrégularités (ex. interventions hors horaires ouvrés).
- L'**évaluation des processus de gestion des accès** (création, modification, suppression, revue périodique).
- Des **recommandations priorisées** selon la criticité.
  - **Présentation des conclusions** à la Direction Générale et/ou au Comité d'Audit.

## **6. Durée de la mission**

- Durée estimée : 6-10 semaines.
- Livraison : rapport provisoire en fin de semaine 8, rapport final en semaine 10 (incluant plan d'actions).

## **7. Livrables**

- Plan de mission validé.
- Rapport provisoire d'audit.
- Rapport final d'audit (incluant plan d'actions).

## **8. Composition de l'équipe d'audit**

- Chef de mission / auditeur principal.
- Auditeur(s) SI spécialisé(s) en IAM.
- Appui éventuel d'un expert en cyber sécurité ou consultant externe.

## **9. Rôles et responsabilités**

Partie prenante	Rôle
Direction Générale	Validation des TDR et des recommandations finales
RSSI	Pilotage de la mission, point de contact
DI	Fourniture des accès, documentation technique
RH / Métiers	Appui sur la revue des rôles et responsabilités
Auditeurs	Réalisation de l'audit, analyse et formulation du rapport

## **10. Confidentialité**

L'ensemble des informations collectées dans le cadre de cette mission est strictement confidentiel. L'équipe d'audit s'engage à respecter les clauses de confidentialité et à sécuriser toutes les données utilisées.

## **ANNEXES**

## **ANNEXE N°1 : Qualification du soumissionnaire**

**Consultation n°25-660 « Mission d'Audit et de Revue des Accès Utilisateurs aux Systèmes d'Information de la Compagnie Tunisienne de Forage (CTF) »**

<b>Critères</b>	<b>Minimum exigé</b>	<b>Réponse du soumissionnaire</b>
Nombre de missions d'audit et de revues des accès utilisateurs aux systèmes d'information, conformes au décret-loi n°2023-17 du 11 mars 2023, réalisées au cours des deux dernières années dans des organismes de taille équivalente à la CTF (effectif supérieur à 100) en Tunisie.	3 missions	
Certification Nationale	Certifié par l'ANCS en cours de validité ou autres	

**Fait à.....le .....**

**Signature et Cachet du soumissionnaire**

**ANNEXE N°2 : Qualification de l'équipe intervenante**

**Consultation n°25-660 « Mission d'Audit et de Revue des Accès Utilisateurs aux Systèmes d'Information de la Compagnie Tunisienne de Forage (CTF) »**

<u>Chef de Projet</u>		
Critères	Minimum exigé	Réponse du soumissionnaire
Diplôme universitaire	Diplôme d'ingénieur en informatique ou réseau ou équivalent	
Certification en audit de sécurité	Certifié par l'ANCS en cours de validité ou autres	
Caractère permanent dans la société (Non contractuel)	Oui (CNSS, etc.)	
Expérience professionnelle en matière sécurité informatique	10 ans	
Nombre de missions d'audit de sécurité (en tant que chef de projet), conformes au décret-loi 2023-17 du 11 mars 2023, effectuées durant les deux dernières années	3 missions	
<u>Un Auditeur</u>		
Critères	Minimum exigé	Réponse du soumissionnaire
Diplôme universitaire	Diplôme d'ingénieur en informatique ou réseau ou équivalent	
Certification en audit de sécurité	Certifié par l'ANCS en cours de validité ou autres	
Caractère permanent dans la société (Non contractuel)	Oui (CNSS, etc.)	
Expérience professionnelle en matière de sécurité informatique, spécialisé en IAM	5 ans	
Nombre de missions d'audit de sécurité, conformes au décret-loi 2023-17 du 11 mars 2023, effectuées durant les deux dernières années	2 missions	

**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).**

Fait à.....le .....

**Signature et Cachet du soumissionnaire**

**ANNEXE N°3 : Fiche des références du soumissionnaire pour des missions de même nature**

**Consultation n°25-660 « Mission d'Audit et de Revue des Accès Utilisateurs aux Systèmes d'Information de la Compagnie Tunisienne de Forage (CTF) »**

Organisme	Objet de la mission	Déroulement de la mission		Responsable du client à contacter	
		DU	AU	Nom	Téléphone

Les missions mentionnées dans le tableau ci-dessus doivent être obligatoirement justifiées par des pièces certifiées conformes (PV de réception ou attestation du client).

Fait à.....le .....

Signature et Cachet du soumissionnaire

**ANNEXE N°4 : Fiche de présentation de l'équipe intervenante**

**Consultation n°25-660 « Mission d'Audit et de Revue des Accès Utilisateurs aux Systèmes d'Information de la Compagnie Tunisienne de Forage (CTF) »**

Nom et Prénom	Diplômes / Certifications	Fonction dans le projet de la CTF

**Fait à.....le .....**

**Signature et Cachet du soumissionnaire**

## ANNEXE N°5 : Modèle de CV des Intervenants

Nom / Prénom :

Niveau universitaire :

Fonction actuelle dans l'entreprise :

Ancienneté dans l'entreprise :

Taches prévues dans la mission :

**1. Diplômes et Certifications :**

Intitulé	Institution	Diplôme / Certificat (fournir pièces justificatifs)	Durée de la formation	Date du diplôme

**2. Missions effectuées en matière de sécurité d'information :**  
(Auditeur SI spécialisé(s) en IAM, Conseil, Etude, etc.)

Organisme	Nature de la mission	Fonction dans la mission	Durée de la mission

Les CVs doivent être légalisés.

Remarque : Le soumissionnaire n'est pas obligé de présenter les CVs de l'équipe intervenante selon le modèle de CV ci-dessus. La CTF accepte les CVs en format libre mais contenant les informations exigées par la CTF.

Fait à ..... Le .....

**L'Intervenant**

(Signature Légalisé)  
(Cachet Obligatoire)

**Soumissionnaire**

## **ANNEXE N°6 : Bordereau des Prix forfait**

Nom du Soumissionnaire ..... :

Désignation	Prix HT En Chiffres	% TVA	Prix TTC En Chiffres
Mission d'Audit et de Revue des Accès Utilisateurs aux Systèmes d'Information de la Compagnie Tunisienne de Forage (CTF)			

**NB :**

Le bureau d'étude doit mentionner le nombre H/J nécessaire pour l'accomplissement de la mission.

**Total en toutes lettres (TTC) :** .....  
.....

Fait à : .....

Le : .....

LE SOUMISSIONNAIRE

Signature et Cachet