PRESIDENCE DE LA REPUBLIQUE

SECRETARIAT GENERAL

Unité de Coordination des Projets (UCP)

Projet d'Appui à la Performance du Secteur Public
(PAPSP)

TERME DE RÉFÉRENCE POUR LE RECRUTEMENT D'UN CABINET POUR ASSURER L'AUDIT DES SYSTÈMES D'INFORMATION DE LA DIRECTION GENERALE DES IMPOTS

1. Contexte

A l'instar de l'évolution numérique et technologique, l'Administration fiscale Malagasy a adopté un plan stratégie 2019 – 2023 axé principalement à la gestion optimale des informations fiscale. Actuellement, la DGI utilise plusieurs systèmes d'informations hétérogènes dans les différentes unités opérationnelles ou fonctionnelles, entre autres :

- SURF, SIGTAS et SAFIRA pour la gestion des dossiers des contribuables, des recettes et des traitements back office ;
- la télé déclaration et Hetraonline : portails Internet permettant de faire la déclaration en ligne, respectivement par les contribuables gérés aux SRE Analamanga et les contribuables gérés dans les autres SRE et les Centres fiscaux ;
- les modules eHETRA, composés de eDeclaration, plateforme de déclaration en ligne utilisée par les contribuables de la DGE, et de ePayment, plateforme de paiement par virement à distance pour les contribuables gérés à la DGE.

Pour permettre d'endiguer les principaux handicaps engendrés par ces systèmes d'information hétérogènes, concernant notamment ses impacts négatifs sur la fiabilité des données et sur l'efficacité des politiques et stratégies fiscales à développer, la DGI accorde une importance capitale à l'implémentation d'un Système d'Administration Fiscale unique et Intégré (SAFI), un chantier en cours.

SAFI sera un système intégré composé de plusieurs modules front office, la suite eHetra et d'un module back office, le SAFI Back office. Les premiers modules front office de la suite eHetra ont déjà été réalisés et déployés auprès de la DGE. Il s'agit du module de paiement, e-Payment, et du module de déclaration e-Déclaration. En plus de ces deux modules, la suite front comprendra, d'une part, la plateforme actuelle d'immatriculation fiscale de la DGI qui

sera conservée, et d'autre part, plusieurs modules front qui vont s'ajouter au fur et à mesure de l'avancement du projet.

La modernisation du Système d'Administration Fiscale requiert des solutions de portée mondiale suivant les normes et standards en vigueur. A cet effet, il est impératif de connaître exactement les forces et les faiblesses des systèmes existants afin de pouvoir mettre en place un nouveau système fiable et répondant concrètement aux besoins des utilisateurs et des autorités.

Dans cette optique, l'évaluation d'un expert externe permettrait de relever les points positifs à considérer et les points négatifs à éviter, dans les systèmes actuels de la DGI pour concevoir et réaliser un SAFI qui s'adapte parfaitement au contexte Malagasy et aux besoins réels des utilisateurs. Pour ce faire, la DGI requiert les services d'un prestataire pour la réalisation d'un audit des systèmes d'informations actuels.

2. Enjeux et objectifs de la mission

La mission a pour but d'analyser le fonctionnement des SI actuels pour en identifier les forces et les faiblesses en termes de performance des applications et de la sécurité des données et des systèmes techniques et matériels.

Cette mission permettra à la DGI de connaître exactement les directives à suivre dans la mise en place du SAFI en termes d'organisation, d'infrastructure et de sécurité informatique.

3. Objet de la prestation

3.1Périmètre

Le consultant fera un audit sur les systèmes informatiques utilisés actuellement par la DGI, spécifiquement, sur les modules front office, à savoir :

- eHetra ;
- HETRAONLINE ;
- HETRAPHONE ;
- et Télédéclaration SIGTAS.

L'audit sera axé sur les domaines ci-dessous et sur les domaines qu'il jugera pertinents et importants pour la réalisation de l'atteinte de l'objectif de sa prestation :

a.L'architecture applicative

Évaluer l'efficacité de l'architecture applicative pour la cohésion des modules, la bonne gouvernance des données, l'interaction avec des systèmes tiers.

b.L'architecture technique

Évaluer la solution technique et son adéquation par rapport aux exigences communes de l'état de l'art en termes de performances, sécurité etc.

c.L'architecture physique

Évaluer l'architecture physique et sa capacité à répondre au niveau de services et aux exigences de sécurité requis.

d. L'architecture opérationnelle

Évaluer l'architecture opérationnelle et sa capacité à répondre aux exigences en termes de supervision, métrologie (recueil et suivi de données de performance), sauvegarde et gestion des environnements (processus et interactions pour le passage entre les différents environnements de la qualification à la production).

3.2 Exigences

- **Identification de l'existant**

  Organiser des entretiens avec les parties prenantes pour identifier les lacunes et les bonnes pratiques déjà en place et d'en sortir la cartographie des données, des informations et des ressources.

- **Test des systèmes informatiques**

  Réaliser différents tests sur les systèmes de la DGI en donnant des références par rapport aux normes et aux bonnes pratiques internationales, notamment :

  - Effectuer des tests de sécurité conformément au guide de test de sécurité Web OWASP (https://owasp.org/www-project-web-security-testing-guide/v42/)
  - Réaliser des tests de piratage social/phising, présenter les résultats et les solutions proposées ;
  - Tester pour s'assurer que le service conserve une disponibilité de 99,95 % et des temps de réponse inférieurs à 100 millisecondes pendant la haute saison, sans relâche excessive pendant les périodes normales, et/ou motiver explicitement tout écart proposé par rapport à cette norme ;
  - Proposer une architecture et des processus spécifiques pour la surveillance et la détection des intrusions.

- **Rapport**

  Rédiger les rapports des entretiens et des tests. Préconisations et propositions de solutions.

4. Résultats attendus et livrables de la mission

Au terme de la prestation, il est attendu du consultant les livrables suivants :

Livrables	**Critères de vérification**
L01 : Plan d'organisation et de réalisation de la mission	Pertinence – Exactitude – Priorité

L02 : Rapport de l'étude de l'existant	Exactitude – Exhaustivité – Pertinence COBIT – ITIL
L03 : Documents contenant : – Le guide des tests de sécurité (préalablement au développement, pendant la conception, pendant le développement, pendant le déploiement, maintenance et opération), – La planification, la découverte et l'exploitation ; – Le rapport des tests de sécurité.	Exactitude – Exhaustivité – Pertinence OWASP
L04 : Document contenant : – Le plan de formation et les scenarios des tests de piratage social/ phishing; – Le guide des tests de simulation de piratage social/ phishing; – Le rapport des tests de simulationcontenant minimalement une description détaillée de chacun de test effectué et des recommandations générales.	Pertinence – Exactitude – Priorité
L05 : Document contenant : – La liste des fonctionnalités, des entrées utilisateurs, des types d'utilisateurs, le tout associé à des scénarios des charges avec le volume que l'on souhaite contrôler (Connexion, transaction, requêtes etc.) ; – Le processus des tests de performance et de la haute disponibilité, le cadrage et l'étude des entrants, le scripting, la modélisation et monitoring et la réalisation des tirs et analyse ; – Le rapport des tests de performance et de la haute disponibilité.	Pertinence – Exactitude – Priorité
L06 : Document d'architecture IDS contenant minimalement : – Le fonctionnement de détection d'attaque (monitoring, analyse et transmission des résultats); – Le diagramme d'IDS – Les avantages et les limites ; – Le système de prévention d'intrusion (IPS) et son fonctionnement ; – La description de processus spécifique de l'IDS et de l'IPS avec les résultats de simulation	Pertinence – Exactitude – Priorité
L07 : Rapport définitif de la mission	Pertinence – Exactitude – Priorité

5. Attendus de la réponse

a. Description de la démarche

Le cabinet devra décrire dans sa réponse la démarche proposée et la synthétiser dans la grille en annexe en décrivant :

- Les étapes
- Pour chaque étape, les livrables proposés et le délai

b. Description et profils du consultant

Le cabinet devra décrire dans la grille en annexe les différents critères concernant son profil

6. Profil du cabinet

Description du poste

L'auditeur de sécurité Informatique et Système d'Information a pour mission d'analyser et de diagnostiquer les systèmes d'information afin de les optimiser et de les rendre plus efficaces.

Missions :

- Analyser le système d'information, évaluer le matériel informatique et l'utilisation de l'informatique ;
- Établir un diagnostic sur le système d'information (technique, organisationnel, économique et humain)
- Analyser les différentes procédures (accès, sécurité, sauvegarde, récupération,…) et leur utilisation
- Identifier les améliorations à apporter, les nouvelles applications à concevoir et les points de sécurité informatique.
- Conseiller et accompagner dans la mise en place ou l'évolution des plateformes d'évaluations logicielles aussi bien les aspects méthodologiques que techniques et opérationnels ;
- Etudier et mener des actions dans l'évolutions et d'amélioration de ces plateformes ;
- Participer à la définition et à la mise en œuvre d'un dispositif permettant d'évaluer la qualité du test et du produit.

Compétences requises

- Le personnel clé du cabinet devrait avoir les compétences suivantes :
- Architecture des systèmes d'information
- Flux d'information dans l'entreprise
- Différents systèmes informatiques
- Principaux modes de communications
- Principaux logiciels des systèmes d'information

- Sécurités SI
- Outils de gestion des exigences, de définition et de gestion de test;
- Cycle de vie d'un SI et de son processus de fabrication;
- Gestion et analyse des risques;
- Modèles d'évaluation et d'évolution des processus;
- Connaissance d'un ou plusieurs domaines fonctionnels;
- Méthodes de génération automatique de tests;
- Langue française (langue de rédaction du rapport)

Activités

- Bâtir une grille d'évaluation et apprécier les résultats obtenus
- Argumenter les décisions prises au regard des résultats et les défendre
- Contrôler les flux d'information dans l'établissement
- Reconnaître les points faibles d'un système d'information
- Concevoir des tests de sécurités

La présente prestation sera assurée par un cabinet qui devrait avoir :

- 10 années d'expériences en Audit organisationnel de systèmes d'information dans les quinze (15) dernières années ;
- 10 années d'expériences en Audit d'architecture informatique et de sécurité informatique dans les quinze (15) dernières années ;
- Avoir réalisé au moins un projet SI dans le domaine de la fiscalité et gestion des finances publiques ;

Le cabinet sera composé de :

- D'un chef de mission
- D'un consultant en sécurité
- D'un consultant en tests de performance

Critères de sélection :

Chef de mission

- Niveau de Formation :Avoir un niveau BAC + 5 en sciences et techniques de l'information, en informatique, ou dans un domaine similaire ;
- Avoir 10 ans d'expériences au moins et une expérience confirmée en matière d'audit de systèmes d'information et audit de sécurité de systèmes d'information ;
- Expériences spécifiques dans le domaine de l'audit des systèmes informatiques, sécurité et réseaux informatiques. Solides connaissances des outils d'évaluation de gouvernance informatique (COBIT 5, ITIL)
- Ayant réalisé au moins une prestation portant sur la rédaction de cahier de charges / réalisation de schéma directeur informatique / élaboration de politique de sécurité / définition de procédures informatiques ;

- Avoir une bonne connaissance des maîtrises d'ouvrage en informatique et Gestion de projet ;
- Expériences dans le domaine d'analyse de risque et d'opportunités et de choix stratégiques ;
- Qualité d'analyse et de rédaction avec une réelle expertise technique ;
- Avoir la capacité prouvée d'assurer le transfert des compétences.

Consultant sécurité

- Niveau de formation : Diplôme d'ingénieur, avec une spécialisation en Sécurité des Systèmes d'Information et informatiques, en réseaux et télécommunication ou en Cryptologie.
- Expériences générales : Forte connaissance en management de la santé sécurité et le rôle de l'audit interne dans celui-ci et maîtrisez des normes ISO 45001 et ISO 19011
- Maîtrise des normes et des procédures de sécurité, des outils et des technologies relatifs à la sécurité informatique (ISO/IEC 27001, COBIT 5, PCI-DSS etc.)
- Solides connaissances des outils d'évaluation et d'analyse de risques (systèmes et réseaux) et des méthodologies (OWASP, EBIOS).
- Qualité d'analyse et de rédaction avec une réelle expertise technique

Consultant expert en tests de performance et de robustesse

- Niveau de formation : Avoir un niveau BAC +5 en informatique ou expérience équivalente ;
- Avoir une expérience d'environ 5 ans en ingénieriede tests de performance et robustesse;
- Ayant réalisé les chantiers et les projets de tests de performance
- Ayant rédigé des plans de tests
- Ayant défini des modèles de charge
- Ayant développé des scripts, notamment des scripts à forte complexité
- Ayant exécuter des campagnes de tirs
- Ayant mis en place du monitoring et analyse des résultats
- Ayant produit des reportings des campagnes de test
- Ayant réalisé des dossiers de capitalisation et d'historisation

7. Durée de la prestation

La prestation durera 10 semaines.

Annexes

A. Grille de description de la démarche

N°	***Intitulé de l'étape***	***Description de l'étape***	***Livrables***	***Délai***
1	*Nom de l'étape*	*Activités à réaliser*	*L01...*	*S0 +1*

B. Grille de description du parcours du cabinet

Domaines	**Description avec expériences selon le domaine**	**Pondération si applicable**
Les références professionnelles	En rapport avec des missions d'audit organisationnel, technique et sécurité du système d'information d'une entreprise ou d'une organisation de même nature	
La qualité du prestataire	CV de l'équipe qui va intervenir pour la mission, avec leur expérience dans des missions d'audit organisationnel, technique et sécurité d'une entreprise ou domaine de même nature ;	
La méthodologie proposée	Modalités, description des outils et méthodes utilisés pour assurer la prestation (déroulement des entretiens...);	
Le calendrier de travail	Calendrier proposé avec le nombre de journées de travail pour réaliser la prestation sur la période définie ;	