THE DANISH INSTITUTE FOR HUMAN RIGHTS

TRUST
Transition Redevable pour la Societe Tunisienne

HAICA
الهيئة العليا المستقلة للاتصال السمعي والبصري

Annexe A

TERMES DE REFERENCES

Mission d'évaluation de la maturité digitale de la Haute Autorité indépendante de la communication audiovisuelle **HAICA**

Juillet 2021

TABLE DES MATIERES

1. Présentation générale

Titre : deux expert(e)s ou prestataire spécialisé pour l'élaboration d'une étude d'évaluation de la maturité digitale

Mission: Evaluation de la maturité digitale de la Haute Autorité indépendante de la communication audiovisuelle HAICA

Organisation : Institut Danois des Droits de l'Homme

Durée de l'étude : jusqu'à 6 mois à partir de la signature du contrat

Nombre de jours de travail : 45 jours

Lieu de travail : Tunis

Langue : l´expert doit être bilingue arabe et français. L´étude sera réalisée en Français.

2. Contexte de la mission

Le projet TRUST appuie les instances publiques indépendantes en tant qu'acteurs principaux dans le système de redevabilité de l'ETAT tunisien. Il vise à améliorer leur positionnement dans le système institutionnel et démocratique tunisien, à travers le renforcement de leur effectivité, de leur accessibilité aux citoyens et de leur capacité à exercer leurs mandats. Le projet TRUST accompagne, dès lors, les instances publiques indépendantes dans leur processus de transformation digitale.

Dans ce cadre, le projet TRUST appuie la Haute Autorité Indépendante de la Communication Audiovisuelle à évaluer le niveau de maturité de son système d'information et de se conformer à la réglementation sécurité en vigueur ainsi qu'à faire une première analyse des pratiques de e-gouvernance/gouvernance électronique de la HAICA.
Le résultat de l'évaluation peut mener à un plan d'action qui permet de remédier aux faiblesses identifiées et d'atteindre un niveau de sécurité adéquat, afin d'assurer une transformation digitale réussie.

3. Objectifs et résultats attendus

L'objet de cette mission est de :

- Définir le niveau de maturité du système d'information de la HAICA

- Réaliser un audit de sécurité réglementaire conformément aux dispositions énoncées dans le décret N°2004-1250 du 25 mai 2004
- Proposer un plan d'action de transformation Digitale et sécurité
- Evaluer le SI après l'intégration des recommandations
- Faire une première analyse des pratiques de e-gouvernance de l'institution et sa conformité avec les principes de la bonne gouvernance dans le but d'identifier les risques et les faiblesses en termes de redevabilité, transparence, participation/autonomisation, non-discrimination (égalité de traitement et groupes vulnérables) et le respect de l'Etat de droit.
- Notamment, il s'agit d'Inclure le respect des droits de l'homme dans l'espace cyber à travers la transformation digitale, par exemple :
    - La Liberté d'expression : l'usage du digital ne doit pas enfreindre les principes de liberté d'expression
    - La Protection des enfants en ligne
    - La Protection des données à caractère personnel et de la vie privée
    - L'aspect accès aux services sans discrimination aussi pour les groupes vulnérables qu'aux marginalisés.

Cette mission doit être menée, tenant compte des exigences **de la norme ISO/IEC 27002 et de la norme ISO 20000 (ITIL)**. Elle doit suivre une approche méthodologique aussi proche que possible de ces référentiels.

La mission devra ainsi concerner les aspects organisationnels, physiques et techniques, relatifs à la sécurité de l'ensemble des entités et moyens (structures, personnel, procédures, outils logiciels, équipements de traitement, équipements réseaux, équipements de sécurité, bâtiments...) en relation avec les fonctions de traitement de l'information et inclus dans le cadre de cet audit.

4. Déroulement de la mission

a. Phase de préparation de la mission :

Il faut préparer tout détail, information ou document nécessaire pour le diagnostic et l'audit, désigner les chefs de projets et les interlocuteurs et fournir les détails complémentaires, relatifs au périmètre de la mission

b. *Phase de sensibilisation :*

Des sessions de sensibilisation préliminaires, et post-audit, destinées aux responsables et acteurs du SI, devront être proposées.

c. *Phase d'évaluation maturité digitale*

Cette phase couvrira un diagnostic basé sur le triple People, process et Technologie.

Inventaire du système d'information

Identifier les différentes composantes du SI HAICA (Infrastructure, application et utilisateurs)

Définition des projets de transformation digitale

Identifier les projets et besoins de transformation digitale de la HAICA tenant compte de la mission de l'organisme et des attentes des parties prenantes.

Il est nécessaire d'adopter une approche participative dans la définition des besoins

Priorisation des projets

Définir une matrice de priorisation des projets identifiés en adoptant une approche participative et rapide en utilisant des techniques de design thinking.

L'évaluation doit porter sur la complexité de réalisation des projets, l'adéquation avec les orientations stratégiques de la HAICA et la capacité de réalisation.

d. *Phase d'audit sécurité :*

Ainsi, cette phase couvrira principalement trois 03 volets :

- Un volet d'audit organisationnel et physique
- Un volet d'audit technique
- Un volet d'analyse et d'évaluation des risques

Volet audit organisationnel et physique

Il s'agit, pour ce volet d'évaluer les aspects organisationnels de gestion de la sécurité de la structure objet de l'audit, d'estimer les risques et de proposer les recommandations adéquates pour la mise en place des mesures organisationnelles et d'une politique sécuritaire adéquate ainsi que des propositions pour l'amélioration de la gouvernance des systèmes.

Audit technique

Il s'agit de procéder à une analyse très fine de l'infrastructure sécuritaire des systèmes d'information et particulièrement du réseau.

Analyse et évaluation du risque :

Dans cette phase et après avoir identifié les failles de sécurité organisationnelles, physiques et techniques, il s'agit de suivre une approche méthodologique pour évaluer les risques encourus et leurs impacts sur la sécurité de la structure auditée.

La phase d'analyse et d'évaluation du risque se déroulera en deux étapes :

i- La phase d'analyse
ii- La phase d'évaluation

e. Synthèse des recommandations

Le titulaire est invité, à la fin de la phase d'audit sur terrain de réaliser 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.

f. Evaluation de l'intégration des recommandations :

Suite à l'intégration des recommandations par l'équipe de la HAICA ou éventuellement par une société tierce, le titulaire devra effectuer des visites à la HAICA afin d'évaluer le bon déroulement de l'intégration de ces recommandations. Cette évaluation se fera suite à une série de visites selon des dates et une planification, organisées après la phase 5 (Synthèse des recommandations) et approuvées par les deux parties.

5. Méthodologie de travail

Pour la réalisation de la mission, le soumissionnaire devra emprunter une approche méthodologique, en indiquant les références de la (ou les) méthodologie(s) adoptées, tout en gardant comme référentiels normatifs la norme ISO/IEC 27002 dernière version et la norme ISO 20000.

Ces méthodologies doivent être adaptées à la réalité, métier et taille de la HAICA

6. Livrables

Deux rapports doivent être livrés :

- Un rapport de diagnostic Digital
- Un rapport d'audit Sécurité SI

a. Rapport de diagnostic Digital

Le rapport de diagnostic doit inclure trois parties :

- Une description et une évaluation complète du système d'information de la HAICA
- Une proposition de projets de transformation digitale en se basant sur le triplet : People, process et technologie et en tenant compte des principes de la bonne gouvernance électronique
- Un plan de mise en œuvre des projets tenant compte des priorités et de la capacité d'exécution de la HAICA

b. Rapport d'audit Sécurité SI

Le rapport d'audit sécurité SI devra couvrir, au minimum, les aspects mentionnés dans le décret N°2004-1250 notamment :

- Une description et une évaluation complète de la sécurité du système informatique, comprenant les mesures qui ont été adoptées depuis le dernier audit réalisé et les insuffisances enregistrées dans l'application des recommandations.
- Une analyse précise des insuffisances organisationnelles et techniques relatives aux procédures et outils de sécurité adoptés, comportant une évaluation des risques qui pourraient résulter de l'exploitation des failles découvertes.
- La proposition des procédures et des solutions organisationnelles et techniques de sécurité qui devront être adoptées pour dépasser les insuffisances découvertes."

Le document final devra inclure les chapitres ou rapports suivants :

- Un rapport détaillé d'audit couvrant les différents aspects spécifiés dans le Cahier des clauses techniques et qui devra comprendre au minimum les sections suivantes :
- Une section relative à l'évaluation des mesures qui ont été adoptées depuis le dernier audit réalisé et des insuffisances enregistrées dans l'application de ses recommandations, avec un report des raisons invoquées par les responsables du SI et celles constatées, expliquant ces insuffisances.
- Une section relative à l'audit organisationnel et physique, fournissant l'ensemble des failles d'ordre organisationnel et physique et incluant la liste des recommandations à

appliquer dans l'immédiat, en tenant compte des spécificités de l'entité, de la classification des systèmes (criticité) et de la réalité actuelle des moyens humains et financiers.

- Une section relative à l'audit technique, indiquant les vulnérabilités existantes, leur impact sur la pérennité des systèmes d'information et de communication de la structure, en incluant des recommandations techniques à appliquer dans l'immédiat, concernant les moyens (réalistes) de correction des failles graves décelées. Tous les travaux de test et d'analyse effectués devront être consignés dans une annexe, en les ordonnant selon leur sévérité, en incluant au niveau du rapport un relevé des plus importantes failles et des moyens de les combler dans l'immédiat.
- Une section relative à la partie analyse des risques fournissant une évaluation des risques résultant des menaces identifiées et des failles découvertes lors des phases d'audit organisationnel, physique et technique.
- Une section relative au plan d'action et stratégie de sécurité à appliquer sur le court terme (jusqu'au prochain audit), comprenant des recommandations précises quant aux mesures à prendre dans le court terme, afin de pallier aux failles et insuffisances décelées, incluant toutes les procédures organisationnelles et techniques en tenant compte pour ce qui concerne le déploiements d'outils et d'architectures de sécurité de l'option d'usage d'outils open-source et de la réalité financière et humaine de l'entité.
- Un rapport présentant le plan d'action cadre s'étalant sur trois années, permettant de mettre en œuvre une stratégie de sécurité cohérente et ciblée. Ce rapport sera mis à jour lors des audits de la seconde et de la troisième année tenant compte du taux de réalisation des mesures qui ont été adoptées depuis le dernier audit réalisé et des insuffisances enregistrées dans l'application de ses recommandations, ainsi que des résultats de l'audit de l'année en cours.
- Un rapport de synthèse, destiné à la direction générale, qui inclura d'une manière claire (destiné aux décideurs) les importants résultats de l'estimation des risques, un résumé succinct des importantes mesures organisationnelles, physiques et techniques préconisées dans l'immédiat et sur le moyen terme (jusqu'au prochain audit), ainsi que les grandes lignes du plan d'action cadre proposé.

7. Qualification et compétences minimale requises de pour la mission

N°	Position	Description	Expérience générale
1	Expert Transformation Digitale	- Diplôme d'Ingénieur Informatique ou Telecom - Expertise en gestion des projets de transformation Digitale - Certifié ITIL ou PMP - Une expérience chez une instance indépendante publique est un plus	Au moins 10 ans
2	Expert auditeur	- Certifié ANSI conformément à l'arrêté du ministre des Technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité informatique,	Au moins 3 ans

La non-conformité à ces critères est éliminatoire

Pièces à fournir

- Les CVs des experts
- Copies des Diplômes
- Certifications (en cours de validité)
- Attestations de formation
- Attestations des clients
- Liste des références et missions réalisées (public et privé)
- Note méthodologique globale
- Planning prévisionnel
- Offre financière en dinar tunisien.
- Pour les **candidatures individuelles** : un acte d'engagement solidaire pour la réalisation de la mission, signé par les deux expert(e)s.
- Et ce document des termes des référenecs, paraphé.

8-METHODOLOGIE DE DEPOUILLEMENT ET ANALYSE DES PROPOSITIONS

Les propositions seront évaluées comme suit :

A- Evaluation technique des Offres :

Nom de la société:		Agence 1-3	
(1) Critère	(2) pondération	(3) points - max 10	(4) Note technique = (2) x (3)
Présentation technique	**30%**		
La structuration de l'offre et la clarté du process	15%	La note attribuée sera la moyenne des notes attribuées par l'équipe de dépouillement	
Expertise dans des projets similaires	15%	La note sera attribuée comme suit : - [10] - l'équipe projet couvre les points suivants : o [5] points : Participation à 3 ou plus de projets de transformation digitale [5] point : Participation à 3 ou plus de missions d'audit sécurité Moins que 3 projets, la note est attribuée selon la règle de trois	
L'adéquation du (des) CV	**70%**		
- Expérience et qualification de l'expert en transformation digitale	35%	La note sera attribuée comme suit : - [8] points: 15 ans d'expérience ou plus - [2] points: une Expertise avec une instance publique indépendante Moins que 15 ans d'expérience, la note est attribuée selon la règle de trois.	
- Expérience et qualification de l'expert cyber sécurité	35%	La note sera attribuée comme suit : - [10] points – 8 ans d'expérience ou plus Moins que 8 ans d'expérience, la note est attribuée selon la règle de trois.	
Résultats	**100%**		

B- Evaluation globale des propositions

Pour la note globale, qui déterminera le rang des offres, l'évaluation technique sera pondérée avec 70%, l'offre financière avec 30%.

Seules les offres ayant obtenues une note supérieure ou égale à 5/10 points seront prises en compte pour la suite de l'évaluation

En cas d'égalité des notes globales, la proposition retenue sera celle dont la proposition technique correspondante a obtenu la meilleure note.

Les offres seront classées par rang.

Le soumissionnaire se réserve droit d'inviter les participants retenus à des présentation de leurs offres et de l'équipe proposée, une note sur 10 points sera attribuée après les présentations, et la note finale sera la moyenne des deux notes

Livrables	Durée estimée (H/J)	TJM	Date début	Date fin
Un rapport de diagnostic Digital				
Un rapport d'audit Sécurité SI				
Total	45			

La note financière sera calculée comme suit :

Note financière = (offre moins disante / offre financière) *10

La note globale est calculée comme suit :

Note globale = (note technique * 0,7) + (note financière * 0,3)

La note finale est calculée comme suit

Note finale = (note globale + Note présentation) / 2