



PRÉSIDENCE DE LA RÉPUBLIQUE

SECRETARIAT GENERAL

Projet de Gouvernance Digitale et de Gestion de l'Identité Malagasy
(PRODIGY)

Unité de Gouvernance Digitale (UGD)

Termes de référence pour le recrutement d'une firme pour l'audit de performance de l'architecture IDMS

1. Contexte

Madagascar s'est engagé dans une réforme structurelle majeure de l'état civil et de l'identité légale, notamment à travers l'adoption de la loi n°2018-027 relative à l'état civil, instituant un identifiant unique de la population. Le système de gestion de l'identité des personnes (IDMS) constitue le socle de l'identité légale et un levier clé pour l'accès des citoyens aux services publics et privés.

Dans ce cadre, une plateforme d'Enregistrement Systématique des Naissances (ESN) est déjà opérationnelle dans plusieurs communes et fait l'objet d'un déploiement progressif à l'échelle nationale. En parallèle, les équipements et solutions nécessaires à l'enrôlement biométrique ont été acquis, permettant la mise en place technique d'un système IDMS intégré.

Toutefois, à ce stade, le système IDMS n'est pas encore entré en phase d'enrôlement massif de la population. Aucun volume significatif de données biométriques ou d'identités n'a encore été enregistré en production. Dans ce contexte, il apparaît nécessaire de conduire un audit pré-enrôlement, visant à évaluer la préparation technique, la posture de sécurité, la gouvernance et la capacité du système à entrer en production dans des conditions maîtrisées, puis un audit de performance opérationnelle basé sur des usages réels.

Cette démarche s'inscrit dans une logique de prévention des risques, de transparence et de renforcement de la confiance des citoyens, en s'assurant que les fondations techniques, organisationnelles et sécuritaires du système sont conformes aux bonnes pratiques internationales avant la création du premier enregistrement citoyen.

2. Objectifs de la mission

2.1 Objectif général

L'objectif général de la mission est de conduire un audit structuré en deux temps complémentaires, couvrant à la fois la phase pré-enrôlement et la phase post-pilote, afin d'évaluer de manière progressive, objective et décisionnelle la sécurité, la capacité, puis la performance réelle du système IDMS.

Cette approche permet de sécuriser le démarrage de l'enrôlement avant la création du premier enregistrement citoyen, puis de valider les performances et la qualité du système sur la base d'usages et de données réelles.

2.2 Objectifs spécifiques

Les objectifs spécifiques sont déclinés selon les deux phases suivantes :

Phase 1 – Audit pré-enrôlement pour

- Évaluer l'architecture technique et fonctionnelle du système IDMS ;
- Apprécier la posture de sécurité et de protection des données personnelles et biométriques ;
- Examiner la capacité théorique, la scalabilité et la résilience du système sur la base d'hypothèses documentées ;
- Évaluer la préparation opérationnelle, organisationnelle et procédurale au lancement de l'enrôlement.

Phase 2 – Audit post-pilote / performance réelle pour

- Mesurer les performances effectives du système en conditions opérationnelles réelles ;
- Évaluer les temps de réponse, le débit, la disponibilité et la résilience observés ;
- Analyser la qualité, l'intégrité et la cohérence des données effectivement collectées ;
- Évaluer l'efficacité des processus opérationnels, incluant les facteurs humains et organisationnels.

3. Périmètre et activités de la mission

3.1 Périmètre

Le périmètre de l'audit couvre l'ensemble des composantes du système IDMS, considérées successivement selon leur état avant et après le démarrage de l'enrôlement pilote, incluant notamment :

- La plateforme d'Enregistrement Systématique des Naissances (ESN) ;

- Les solutions et équipements d'enrôlement biométrique ;
- Les infrastructures centrales et les réseaux de communication ;
- Les interfaces utilisateurs et outils d'administration ;
- Les dispositifs de sécurité logique et organisationnelle ;
- Les procédures d'exploitation, de sauvegarde, de continuité et de gestion des incidents ;
- Les mécanismes d'interopérabilité avec les systèmes existants.

3.2 Activités par phase

Phase 1 – Pré-enrôlement :

- Revue documentaire et entretiens avec les parties prenantes ;
- Documentation de l'architecture et analyse des risques ;
- Audit de sécurité et de protection des données ;
- Tests de charge et de performance sur la base de scénarios synthétiques explicitement définis ;
- Évaluation de la préparation opérationnelle et organisationnelle.

Phase 2 – Post-pilote :

- Analyse des journaux, métriques et données générées en conditions réelles ;
- Mesures objectives des performances observées (temps de réponse, débit, disponibilité) ;
- Analyse de la qualité des données biographiques et biométriques ;
- Évaluation des workflows terrain, de la déduplication et de l'adjudication ;
- Identification des goulots d'étranglement techniques, humains et organisationnels.

4. Référentiels et critères d'audit

L'audit sera conduit sur la base de critères explicites et documentés, incluant notamment :

- La loi n°2014-038 relative à la protection des données à caractère personnel à Madagascar, et ses textes d'application ;
- ISO/IEC 27001 – Système de management de la sécurité de l'information ;
- ISO/IEC 27701 – Management de la protection des données personnelles ;
- ISO/IEC 24745 – Protection des données biométriques ;
- NIST SP 800-63 – Digital Identity Guidelines (principes applicables) ;
- Principes de la Banque mondiale – ID4D ;
- Principes fondamentaux du RGPD, à titre de bonnes pratiques internationales ;
- Convention de Malabo sur la cybersécurité et la protection des données personnelles.

Une matrice de conformité et une grille d'évaluation seront utilisées afin d'objectiver les conclusions (conforme / partiellement conforme / non conforme).

5. Résultats attendus et livrables

Les résultats et livrables attendus sont structurés de manière progressive, en cohérence avec les deux phases de l'audit.

Livrables – Phase 1 (pré-enrôlement) :

- Plan d'audit détaillé validé en début de mission ;
- Description de l'architecture ;
- Rapport d'audit pré-enrôlement incluant les constats techniques et organisationnels, la matrice des risques priorisés, l'évaluation de conformité aux référentiels retenus et les recommandations conditionnant le démarrage de l'enrôlement pilote.

Livrables – Phase 2 (post-pilote) :

- Rapport d'audit de performance réelle et de qualité des données ;
- Analyse comparative entre capacités projetées et performances observées ;
- Recommandations d'optimisation technique, organisationnelle et opérationnelle ;
- Avis argumenté sur le passage à l'enrôlement à grande échelle.

Une synthèse exécutive consolidée sera produite à l'issue des deux phases à destination des décideurs.

6. Profil et qualifications de la firme

La firme devra justifier d'une expertise avérée en audit de systèmes d'identité numérique et de systèmes critiques, incluant les technologies biométriques et la sécurité de l'information. Une expérience confirmée dans des audits pré-production de systèmes nationaux d'identité est requise. Les experts proposés devront également justifier d'une expérience internationale et/ou des experts locaux disposant d'une expérience internationale significative dans ce type de mission.

L'équipe devra inclure au minimum :

- Un chef de mission senior expert en systèmes d'identité numérique ;
- Un auditeur certifié en sécurité de l'information et protection des données ;
- Un expert en architecture et infrastructures critiques ;
- Un expert en gouvernance et préparation opérationnelle.

7. Durée de la mission

La mission s'étendra sur une durée maximale de trois (3) mois, incluant les phases de cadrage, d'audit technique et organisationnel, et de restitution des résultats.

L'exécution de la mission se déroulera principalement à Antananarivo où se trouve le siège de l'institution en charge de l'état civil et de l'identité, avec des déplacements sur des sites de déploiement sélectionnés sur le territoire national pour évaluer l'implémentation en conditions réelles.

8. Evaluation des offres

Les soumissionnaires devront présenter une offre technique détaillée attestant leur compréhension des enjeux de la mission et de l'approche méthodologique proposée. Ils devront également fournir les curriculum vitae détaillés des membres de l'équipe mobilisée, les certificats, références et attestations de missions similaires, ainsi qu'une offre financière détaillée. L'ensemble des pièces justificatives, attestations et certifications permettant d'établir les qualifications et l'éligibilité du cabinet devra aussi être joint au dossier de soumission.