PRÉSIDENCE DE LA REFONDATION DE LA RÉPUBLIQUE

SECRETARIAT GENERAL

PROjet de Gouvernance DIgitale et de Gestion de l'Identité MalagasY
(PRODIGY)

Unité de Gouvernance Digitale (UGD)

Computer Incident Response Team (CIRT)

CONSTITUTION D'UNE BASE DE DONNÉES DE CABINETS D'AUDIT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

May 2026

Référence	CIRT/AUDIT-SSI/2026/001
Autorités mandataires	CIRT-Mdg
Responsable CIRT-Mdg	Head Manager of CIRT
Objet de la mission	Constitution d'une base de données de cabinets d'audit en sécurité des systèmes d'information
Date de publication	26/05/2026
Date limite de soumission	30/06/2026
Langue de soumission	Français

1. Contexte et justification

1.1 Mandataire

Le Computer Incident Response Team de Madagascar (CIRT-Mdg) est l'autorité mandataire du présent du présent avis de recensement . Équipe nationale de réponse aux incidents de cybersécurité, le CIRT-Mdg est l'organe chargé de la coordination et de la gestion des incidents de cybersécurité au niveau national,notamment :

- La détection, l'analyse et la coordination de la réponse aux incidents cyber affectant les infrastructures critiques de l'État ;
- La veille sur les cybermenaces et la diffusion d'alertes et de bulletins de sécurité aux entités gouvernementales ;
- Le renforcement des capacités des équipes techniques des ministères en matière de cybersécurité ;
- La coopération avec les CERT/CSIRT régionaux et internationaux (AfricaCERT, FIRST, etc.) ;
- L'élaboration et la mise à jour des procédures nationales de gestion des incidents de cybersécurité.
- La coordination des audits de sécurité des systèmes d'information de l'État et la supervision de la mise en œuvre des recommandations qui en découlent.

C'est dans l'exercice de cette dernière attribution que le CIRT-Mdg lance le présent AMI, en vue d'identifier des cabinets d'audit spécialisés aptes à évaluer de manière indépendante et rigoureuse le niveau de sécurité des systèmes d'informations.

1.2 justification de la mission

Dans un contexte international marqué par l'intensification des cybermenaces (rançongiciels, espionnage, fuites de données) et dans le cadre de la mise en œuvre de la Stratégie Nationale de Cybersécurité de Madagascar, le CIRT-Mdg souhaite constituer une base de données nationale de cabinets qualifiés en audit de sécurité des systèmes d'information.

Cette base de données servira de référentiel pour :

- les OIV et autres institutions publique pour leur propre audit interne en SSI
- les prestations d'audit SSI à réaliser auprès des OIV et institutions publiques sur demande des autorités

1.3 Périmètre général des compétences recherchées

Les cabinets retenus pourront être sollicités ultérieurement pour intervenir sur les domaines suivants :

- Gouvernance et politique de sécurité des SI
- Infrastructures réseaux et télécoms
- Tests d'intrusion (pentest)
- Sécurité des serveurs, systèmes et bases de données
- Sécurité des applications e-gouvernement
- Gestion des identités et des accès (IAM/PAM)
- Continuité d'activité et sauvegardes
- Conformité réglementaire et normes internationales
- Sensibilisation et maturité en cybersécurité

2. Objectif

Le présent Appel vise à constituer une liste de référence de cabinets d'audit qualifiés en cybersécurité, susceptibles d'être consultés dans le cadre de futurs appels d'offres restreints ou missions spécifiques.

Cette base de données permettra au CIRT-Mdg de disposer d'un vivier de prestataires compétents répondant aux standards internationaux.

3. Critères d'Éligibilité et de Qualification

3.1 Conditions générales d'éligibilité

- Etre un cabinet d'audit ou une société de conseil en cybersécurité légalement constitué(e) dans son pays d'établissement
- Etre en règle vis-à-vis de l'ensemble des obligations légales, fiscales et sociales de son pays d'établissement ;
- Ne pas être sous le coup d'une procédure de liquidation judiciaire, de redressement ou de faillite ;
- Ne pas être inscrit sur une liste d'exclusion des marchés publics nationaux ou internationaux
- Ne présenter aucun conflit d'intérêt direct ou indirect avec le CIRT Mdg ou ses partenaires.

3.2 Capacités techniques et expérience

- Justifier d'au moins cinq (5) années d'expérience documentée dans le domaine de l'audit de sécurité des systèmes d'information ;

- Avoir réalisé au minimum trois (3) missions d'audit SSI de nature similaire au cours des cinq (5) dernières années, idéalement pour des institutions publiques ou parapubliques ;
- Disposer d'une équipe pluridisciplinaire d'auditeurs qualifiés couvrant : la sécurité offensive (pentest), la sécurité réseau et infrastructure, la sécurité applicative, la gouvernance et conformité SSI ;
-

3.3 Certifications requises ou appréciées

Les auditeurs-clés proposés pour la mission devront justifier d'au moins une (1) des certifications suivantes :

- CISA – Certified Information Systems Auditor (ISACA) ;
- CISSP – Certified Information Systems Security Professional (ISC²) ;
- CEH – Certified Ethical Hacker (EC-Council) ;
- OSCP – Offensive Security Certified Professional (OffSec) ;
- ISO/IEC 27001 Lead Auditor et Lead Implementer ;
- GIAC (GSEC, GPEN, GWAPT, GCIH, etc.) ou certifications équivalentes reconnues.
- ITIL Foundation

3.4 Exigences de confidentialité, sécurité et intégrité

Compte tenu du niveau de sensibilité des informations auxquelles les auditeurs auront accès, le cabinet devra impérativement :

- Signer un Accord de Non-Divulgation (NDA) spécifique avant tout accès aux systèmes et aux données ;
- Garantir que l'ensemble du personnel affecté à la mission a fait l'objet d'une vérification approfondie des antécédents (casier judiciaire, références professionnelles) ;
- S'engager à ne communiquer aucune information relative à la mission à des tiers non autorisés
- N'utiliser les accès techniques accordés qu'aux strictes fins de l'audit, dans le cadre temporel défini ;
- Respecter les procédures de sécurité opérationnelle définies par le CIRT Mdg lors de toutes les phases de l'intervention.

4. Composition du Dossier de référencement

4.1 Documents administratifs

- Lettre de manifestation d'intérêt adressée au Head Manager du CIRT Mdg signée et cachetée par le représentant légal du cabinet ;
- Copie des statuts de la société, extrait du registre de commerce ou équivalent (moins de 3 mois) ;
- Attestation fiscale en cours de validité et attestation de régularité des cotisations sociales ;
- Attestation de non-faillite et de bonne situation juridique délivrée par l'autorité compétente
- Déclaration sur l'honneur attestant de l'absence de conflit d'intérêts et de non-exclusion des marchés publics.

4.2 Documents techniques

- Note de présentation du cabinet : historique, organisation, domaines d'expertise SSI – 5 pages maximum ;
- Références détaillées d'au minimum trois (3) missions d'audit SSI comparables réalisées au cours des cinq (5) dernières années : nom du client (si non confidentiel), nature et périmètre de la mission, durée, résultats obtenus, coordonnées de référence pour vérification
- CV détaillés des auditeurs-clés proposés pour la mission, précisant : formations académiques, certifications professionnelles, années d'expérience et principales missions réalisées ;
- Copies des certifications professionnelles des auditeurs mentionnés ;
- Note méthodologique (5 à 10 pages) décrivant l'approche, les phases, les outils envisagés et la démarche qualité pour la conduite de l'audit SSI ;
- Liste et description des outils et logiciels d'audit utilisés (scanners de vulnérabilités, plateformes de pentest, outils d'analyse forensique, etc.).

5. Modalités de Soumission

5.1 Format de soumission

Les dossiers doivent être soumis sous double enveloppe fermée. L'enveloppe extérieure ne doit comporter aucun signe d'identification du soumissionnaire. Elle doit obligatoirement porter la mention suivante :

« CONSTITUTION D'UNE BASE DE DONNÉES DE CABINETS D'AUDIT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION – AUDIT SSI
Réf. CIRT/AUDIT-SSI/2026/001
– À N'OUVRIR QU'EN SÉANCE D'ÉVALUATION »

Chaque dossier devra comprendre :

- Un (1) exemplaire original papier, clairement identifié « ORIGINAL » ;
- Une (1) copie numérique sur clé USB chiffrée — le mot de passe devra être transmis séparément par email à l'adresse dédiée ci-après.

5.2 Adresse de dépôt

Destinataire	Monsieur le Head Manager of CIRT
Institution	CIRT Mdg
Adresse physique	Village des Jeux Ankorondrano, Bâtiment D1, Antananarivo 101, Madagascar.
Email	head.manager@cirt.gov.mg, contact@cirt.gov.mg
Téléphone	+261 34 80 694 34

5.3 Date limite de soumission

⚠ **Date limite absolue : [30/06/2026] à 17h00 (heure locale – Antananarivo).**

Tout dossier reçu après ce délai sera automatiquement rejeté, sans examen et sans examen préalable et sans possibilité de recours . Aucune prorogation ne sera accordée.

6. Évaluation des Dossiers et Constitution de la Liste Restreinte

Les dossiers de manifestation d'intérêt seront examinés et évalués par un Comité d'Évaluation constitué au sein du CIRT Mdg, selon les critères ci-après :

Critère d'évaluation	Pondération (%)	Note max.
Expérience générale en audit de sécurité des SI (≥ 5 ans)	**20%**	**20**
Références de missions similaires réalisées (≥ 3 missions documentées)	**25%**	**25**
Qualifications et certifications des auditeurs-clés	**25%**	**25**
Qualité de la note méthodologique et approche technique proposée	**20%**	**20**
Moyens techniques disponibles (outils d'audit, infrastructure de pentest)	**10%**	**10**
total	**100%**	**100**

Seuil minimum de présélection : 70 points sur 100.

Le CIRT Mdg se réserve le droit de :

- Contacter les clients référencés par les candidats pour vérification des informations déclarées ;
- Solliciter des clarifications ou des compléments d'information auprès des candidats présélectionnés ;
- Convoquer les candidats présélectionnés pour une présentation orale de leur approche avant la constitution de la liste restreinte finale ;
- Retenir jusqu'à cinq (5) cabinets sur la liste restreinte finale.

Les candidats retenus sur la liste restreinte seront informés par écrit. Les candidats non retenus pourront demander un retour succinct sur leur dossier.

7. Dispositions Générales

- Le présent document ne constitue pas un appel d'offres et n'engage pas le CIRT Mdg dans l'attribution d'un marché ;
- La participation à cet appel ne confère aucun droit automatique à la conclusion d'un contrat ;
- Le CIRT Mdg se réserve le droit de modifier, de suspendre ou d'annuler le présent AMI à tout moment et sans recours ;
- Les frais de préparation, d'impression et de soumission du dossier sont à la charge exclusive du candidat ;

- Toute tentative d'influence, de corruption ou de fraude entraînera la disqualification immédiate et définitive du candidat, et pourra faire l'objet de poursuites judiciaires conformément à la législation malgache ;
- Les informations communiquées dans les dossiers seront traitées de manière strictement confidentielle et utilisées aux seules fins d'évaluation par le CIRT Mdg ;
- Le CIRT Mdg n'est pas tenu de restituer les dossiers de candidature soumis ;

Point focal	Eric RAKOTOMANIRAKA
Structure	CIRT Mdg
Email dédié	head.manager@cirt.gov.mg, contact@cirt.gov.mg
Téléphone	+261 34 80 694 34

Important : Les questions doivent obligatoirement être soumises par écrit, au plus tard dix (10) jours ouvrables avant la date limite de soumission. Les réponses seront communiquées simultanément à l'ensemble des candidats ayant retiré le dossier, sans indication de l'auteur de la question.