REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

FONDS SPECIAL D'EQUIPEMENT ET D'INTERVENTION INTERCOMMUNALE

AVIS DE SOLLICITATION A MANIFESTATION D'INTERET N°09/ASMI/FEICOM/DG/2025
DU 14 FEV 2025

POUR LE RECRUTEMENT D'UN CONSULTANT INDIVIDUEL EN VUE DE L'ELABORATION D'UN PLAN DU CONTINUITE DE L'ACTIVITE ET D'UN PLAN DE REPRISE SUR INCIDENT IT DU FEICOM – EXERCICE 2025

1-CONTEXTE ET JUSTIFICATION

La modernisation de la gestion du Fond Spécial d'Equipement et d'Intervention Intercommunal (FEICOM) est depuis plusieurs années, un des objectifs majeurs de l'organisme, d'où son inscription dans les différents documents de planifications. En effet, à la suite de plusieurs audits institutionnels, des recommandations fortes avaient été faites à l'équipe de gestion du FEICOM dans ce sens. En vue d'y apporter des solutions, l'entreprise a adopté une approche innovante de management en mettant en place notamment les Systèmes de Management de la Qualité et Environnemental, le Contrôle de Gestion, l'Audit Interne et l'Approche Risques.

Au niveau du Système d'Information (SI), plusieurs outils ont été déployés dès 2015 : l'ERP (Enterprise Ressources Planning) baptisé Axiome Solution FEICOM (ASOFEI), l'interconnexion de la Direction Générale avec les Agences Régionales, la téléphonie IP, la messagerie collaborative, etc.

Dans le souci de garantir la continuité des activités fortement dépendantes de son Système d'Information majoritairement digitalisé, il devient urgent pour le FEICOM de se doter d'un plan de continuité de l'ensemble de ses activités (PCA), afin de garantir la non interruption de ces dernières, celles-ci étant génératrices de valeurs. Le Plan de Reprise sur l'Incident (PRI) qui accompagne le premier, permettra à l'organisme de définir des actions de relance progressive des services informatiques en tenant compte de leur criticité et de nombreux paramètres techniques et organisationnels.

En vue d'y parvenir, le FEICOM a commencé par une étude lui permettant d'évaluer l'impact actuel de la digitalisation sur son fonctionnement. Cette approche offre l'avantage de donner à l'organisme une meilleure lisibilité sur le rapport entre les processus métiers et les outils numériques qui les porte. En plus, il identifie différents scénarios de risques et leur impact sur l'organisme en cas de crise ou de sinistre. Ces éléments servent d'entrée au processus d'élaboration du PCA/PRI.

Cette étude préalable étant faite, le FEICOM souhaiterait passer à l'étape suivante relative à l'élaboration des outils cités supra. Dans ce sens, il est envisagé le recrutement d'un consultant individuel, expert en la matière pour accompagner l'organisme dans cette phase du projet.

2. OBJECTIF DE LA PRESTATION

A travers l'élaboration d'un plan de continuité d'activité (PCA) et d'un Plan de Reprise sur Incident (PRI), le FEICOM a pour objectif de décliner une stratégie et un ensemble de dispositions pour garantir la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement. La finalité ici étant de réduire au maximum l'impact d'une crise liée au SI sur la mise en œuvre des missions de l'organisme. Ceci peut se traduire par les objectifs spécifiques suivants :

- Définir une stratégie de continuité des services et de reprise, sur la base des résultats de l'étude d'impact sur l'activité réalisée précédemment.

- Proposer un ensemble d'outils et de procédures visant à garantir, en cas de sinistre, la disponibilité des activités majeures du FEICOM.

- Définir les architectures d'infrastructure et applicatives optimales pour la reprise et la continuité des services.

- Proposer un ensemble d'outils et de procédures à suivre afin de redémarrer le système informatique dans les meilleurs délais, et avec le minimum de perte de données, suite à un sinistre.

- Sensibiliser et former les différents acteurs aux outils implémentés.
- Transférer les compétences aux personnels de la CSI qui devront assurer le relais.

3. NATURE ET CONSISTANCE DES PRESTATIONS

D'un point de vue opérationnel, les résultats suivants sont attendus de la mise en place du présent projet.

- **Un meilleur alignement du SI sur les éléments de contexte de l'organisme :** par la description des objectifs et des obligations de l'entreprise, dont va découler la liste des activités essentielles pour les accomplir. Cette liste s'accompagne des différents processus nécessaires au fonctionnement desdites activités.
- **Une approche méthodologique et structurée de réponse aux risques les plus critiques :** le PCA/PRI permet d'identifier quels sont les risques les plus graves pour la continuité des activités essentielles, accompagnés de plusieurs scénarios quant à leur survenance.
- **L'identification des rôles et responsabilités en cas de crise :** le PCA/PRI met en place une organisation qui identifie les différentes personnes responsables, leur rôle et les procédures de la mise en œuvre du PCA, accompagnés des moyens associés pour pouvoir l'exécuter.
- **Une meilleure gestion de crise :** l'opérationnalisation du PCA/PRI permet de définir les procédures de détection d'incident, de qualification, d'escalade, d'alerte, de mobilisation ou encore d'activation de la cellule de crise ainsi que des seuils de déclenchement des mesures du PCA et la communication associée.
- **La maintenance opérationnelle du PCA/PRI permet de maintenir l'entreprise en éveil.**

Au niveau stratégique la mise en place d'un PCA/PRI contribuera à la performance du FEICOM à plus d'un titre :

- *Au niveau financier* : le maintien des résultats financiers, l'anticipation de nouvelles dépenses induites par les crises ;
- *Au niveau de la relation client* : le maintien de la confiance des clients et des partenaires, ainsi que des donneurs d'ordres et autres parties intéressées ;
- *Au niveau de la conformité* : le respect des obligations légales et contractuelles ;
- *Au niveau de l'image et de la responsabilité* : le PCA/PRI est une preuve de bonne gouvernance qui va accroître la visibilité de l'organisme et maintenir la confiance auprès des parties prenantes.

4. METHODOLOGIE

L'atteinte des objectifs cités plus haut, se fera par la mise en œuvre d'actions spécifiques, matérialisées par la production de livrables à chacune des étapes.

Ces actions pourraient se présenter en trois principales étapes que sont l'élaboration du plan de continuité de l'activité (PCA), l'élaboration du plan de reprise sur incident (PRI) ainsi que la Formation et le transfert de compétences bau personnel du FEICOM indiqué.

#	ACTIVITES	DESCRIPTION	LIVRABLES
ETAPE 1 : Plan de Continuité de l'Activité (PCA)			
1	Appropriation et exploitation des éléments de sortie du BIA	Il s'agira d'analyser les livrables du BIA, d'en ressortir les éléments de contexte, identifier les risques, identifier les conséquences sur les activités ainsi que les mesures.	- Proposition du périmètre du PCA - Analyse des exigences vis-à-vis des parties intéressées - Cartographie des risques optimisés - Mise à jour des livrables du BIA (Objectifs de Points de Récupération (RPO), Objectifs de Temps de Récupération (RTO), etc.)
2	Définition de la stratégie de continuité des activités	Elle permet de formaliser les mécanismes de continuité d'activité pour s'assurer que les activités critiques du périmètre puissent être menées en cas d'incident grave sur la SI. Elle va permettre de définir un niveau minimal de service acceptable pour la CSI, afin de garantir l'atteintes des objectifs des métiers en cas de dysfonctionnement.	- Listing des scénarii de risque à mitiger, et plan de réponse correspondant - Stratégie de continuité des activités en alignement avec celle de l'organisme et avec les objectifs des processus métiers.
3	Elaboration des outils de mise en œuvre et d'évaluation du PCA	Cette activité va consister à concevoir des outils (techniques, organisationnels, méthodologiques, etc.) pour la mise en œuvre d'u PCA. De même il s'agira d'élaborer des indicateurs d'évaluation, des procédures de tests et des mécanismes d'optimisation du PCA. Enfin des vérifications devront être effectuées pour s'assurer de la conformité réglementaire du PCA (code du travail, règlements sur la propriété intellectuelle, etc.).	- Procédures et instructions de travail pour la continuité - Procédure de gestion de crise (Comité de crise, Rôles et responsabilités des acteurs) - Plan de communication de crise - Cellule de veille des incidents IT et instructions de travail - Proposition d'outils ou de technologies adaptés à l'environnement technique du FEICOM et aux exigences normatives.
ETAPE 2 : Plan de Reprise sur Incident (PRI)			
4	Définition de la stratégie de Reprise sur Incidents	Elle permet de formaliser les mécanismes de fonctionnement en modes dégradés et de reprise technique, d'identifier au préalable les priorités, de définir le niveau de service à restaurer et les délais associés. Elle va également permettre l'identification préalable de l'ordre de priorité de reprise et de basculement progressif sur les systèmes normaux (site informatique, bâtiment, etc.)	- Listing des scénarii de risque à mitiger identifiés, et plan de reprise correspondant - Stratégie de reprise des activités en alignement avec celle de l'organisme et avec les objectifs des processus métiers.
5	Elaboration des outils de mise en œuvre et d'évaluation du PRI	Des outils techniques et organisationnels (équipements, architecture technique, procédure, etc.) devront au cours de cette activité être proposés en vue de l'optimisation des mécanismes de sauvegardes de données, de restauration(architecture et équipements, site de reprise) et de tests de reprise sur incident IT.	- Procédure de sauvegarde optimisées - Procédure de restauration - Procédure de tests de reprise - Architectures techniques et outils de reprise - Proposition d'équipements pour backup - Proposition de site de reprise
Etape 3 : Formation et transfert de compétences			
6	Communication et Sensibilisation sur le PCA/PRI	- La sensibilisation des responsables de structures aux notions de continuité et de reprise des activités - L'appropriation des points focaux des plans de continuité et de reprise élaborés	- Plan de communication et sensibilisation - Supports de sensibilisation et communication (flyers, mini vidéos, etc.) - Supports de formation.

7	Formation et transfert des compétences techniques	Transfert de compétence et formation des responsables de la CSI à l'appréciation et au traitement des risques, ainsi qu'à la continuité des services IT	-Supports de formation -Certificats de formation

5. PROFIL DU CONSULTANT

Les consultants postulants doivent réunir les conditions suivantes :

- Spécialisation dans la mission :
  - Détenir un agrément à jour de l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) pour les audits des SI ;
  - Détenir un agrément à jour des organismes de certification pour la mise en place et l'audit de certification des SI aux normes ISO dans l'un des domaines ci-après :
    - Système de Management de la Sécurité de l'Information ;
    - Système de Management de la continuité de l'activité ;
    - Système de Management de la gestion des Risques de l'Information.
  - Etre un consultant expert dans les domaines suivants : Gouvernance de l'Information, Risques, Gestion de la Sécurité de l'Information, cyber sécurité, enquêtes cybernétiques et stratégie de cyberdéfense.
- Justifier des qualifications ci-dessous répertoriées :
  - Expérience dans les missions de mise en place de dispositifs de gouvernance SI : justifier de sept (07) ans au moins dans l'élaboration de stratégies, politiques, procédures et manuels dans les domaines de la sécurité de l'information et de la gouvernance des données (présenter justificatifs des projets menés) ;
  - Expérience dans les missions d'implémentation des SMSI : justifier d'au moins 03 missions d'implémentation des Systèmes de Management de la Sécurité de l'Information (SMSI) sur les cinq dernières années ;
  - Expérience dans les missions d'audit des SMSI : justifier d'au moins 03 missions d'audits de sécurité et d'évaluation des risques cybernétiques sur les cinq dernières années ;
  - Expérience dans les missions d'accompagnement ou d'implémentation des PCA/PRI : justifier d'au moins une mission d'implémentation d'élaboration et/ou d'implémentation d'une stratégie *Data Protection and Data Recovery*, sur les trois dernières années ;
  - Expérience dans les missions de cyber sécurité, cyberdéfenses et enquêtes cybernétiques ; apporter la preuve d'avoir mené au moins trois enquêtes cybernétiques d'envergure (pour une organisation d'au moins 150 employés) dans les deux dernières années ;
  - Qualifications du consultant
    - Qualifications pour la mission (au minimum bac +5) en management des organisations, gestion des systèmes d'information, ou tout autre diplôme équivalent (CV détaillé, et copies de diplômes, etc.) ;
    - Certifications requises pour la mission, au moins quatre des huit ci-après :
      - ✓ Une certification ISO 27001 V2022, Lead auditor,
      - ✓ Une certification ISO 27001 V2022, Lead implementer,
      - ✓ Une certification ISO 27005 V2018,
      - ✓ Une certification EC-Council Incident Handling (ECIH V2),
      - ✓ Une certification EC-Council Computer Hacking Forensic Investigator (CHFI),
      - ✓ Une certification EDRP V3,
      - ✓ Une certification CEH (Ethical Hacking),
      - ✓ Une certification CDPO (Certified Data Protection Officer).

6. CRITERES DE QUALIFICATION OU D'EVALUATION

Pour le Dossier Administratif, les pièces administratives suivantes sont requises :

- Une lettre de manifestation d'intérêt timbrée ;
- Une attestation de non exclusion des marchés publics délivrée par l'ARMP ;
- Une copie certifiée de la carte de contribuable ;
- Attestation et plan de localisation certifiés.

** NB : Toutes les pièces fiscales devront être datées de moins de trois mois.*

Pour le Dossier Technique, les documents ci-dessous doivent être produits *:*

a) Chaque Consultant fournira :

Un dossier de références techniques présentant les documents certifiant la spécialisation du consultant pour la mission :

- Agrément ANTIC ;
- Agrément pour la mise en place et l'audit de certification aux normes ISO exigées ;
- Expertise dans les domaines de la mission.

Un dossier d'Expérience du Consultant (Références du Consultant Qualification et Compétences

- Expérience dans les missions de mise en place de dispositifs de gouvernance SI : ;
- Expérience dans les missions d'implémentation des SMSI ;
- Expérience dans les missions d'audit des SMSI ;
- Expérience dans les missions d'accompagnement ou d'implémentation des PCA/PRI ;
- Expérience dans les missions de cyber sécurité, cyberdéfenses et enquêtes cybernétiques ;

Un dossier comprenant les Qualifications du consultant ;

- Qualifications pour la mission (CV, et copies de diplômes, etc.) ;
- Certifications requises pour la mission (2 points par certification exigées) ;
- Méthodologie et compréhension de la mission.

7. CRITERES D'EVALUATION DU DOSSIER TECHNIQUE

Critères d'évaluation	Répartition	Points	
		Nombre	Sous total
PRESENTATION GENERALE	Format	1,5 pts	05 pts
	Respect de l'ordre des pièces	1,5 pts	
	Intercalaires	2 pts	
REFERENCES TECHNIQUES DU CONSULTANT	Agrément ANTIC ;	5 pts	15 pts
	Agrément pour la mise en place et l'audit de certification aux normes ISO exigées ;	5 pts	
	Expertise dans les domaines de la mission.	5 pts	
EXPERIENCE DU Consultant (Références du Consultant Qualification et	Expérience dans les missions de mise en place de dispositifs de gouvernance SI : 10% ;	10	50 pts
	Expérience dans les missions d'implémentation des SMSI : 10% ;	10	

Compétences Justifier les contrats	Expérience dans les missions d'audit des SMSI : 10% ;	10	
	Expérience dans les missions d'accompagnement ou d'implémentation des PCA/PRI : 10% ;	10	
	Expérience dans les missions de cyber sécurité, cyberdéfenses et enquêtes cybernétiques : 10%.	10	
QUALIFICATIONS DU CONSULTANT	Diplômes certifiés plus CV signé et daté	5	10 pts
	Certifications requises pour la mission (2 points par certification exigées)	5	
METHODOLOGIE ET PLANNING D'EXECUTION DES PRESTATIONS ET COMPREHENSION DE LA MISSION	Méthodologie d'intervention : *Bonne (12 pts) *Moyenne (08 pts) * Faible (05 pts)	12 pts	20 pts
	Planning d'exécution conforme à la méthodologie : *Bonne (04 pts) *Moyenne (2 pts) *Faible (01 Pts)	4 pts	
	-*Bonne compréhension (04 pts) *Compréhension Moyenne (2 pts) *Faible compréhension (01 Pts) (au moins 3 observations)	4 pts	
TOTAL			100 pts

Seules les offres techniques ayant obtenu 80 points ou plus des points ouvriront droit à l'examen des offres financières.

8. DUREE DE LA MISSION

La présente mission devra être exécutée dans un délai de cent vingt (120) jours ouvrés. Ces délais sont automatiquement suspendus durant les phases de validation des livrables.

Des ordres de service seront notifiés par l'Ingénieur du Marché à la fin de chaque période. Les rapports provisoires seront produits et validés dans les sept (07) jours suivant la réception et le rapport final dans les quatorze (14) jours maximums.

9. FINANCEMENT

Les prestations objet du présent Avis de sollicitation à manifestation d'intérêt seront financées par le budget du Fonds Spécial d'Equipement et d'Intervention Intercommunale, Exercice 2025.

10. MENTION A INSCRIRE :

Les dossiers de manifestation d'intérêt devront parvenir en cinq (05) exemplaires en français ou en anglais, sous pli fermé et scellé, à l'adresse ci-après, au plus tard le 07 MAI 2026 à 10 heures, avec la mention suivante :

« AVIS DE SOLLICITATION A MANIFESTATION D'INTERET N°003/ASMI/FEICOM/CIPM/2025 DU 13 A FEV 2025 POUR LE RECRUTEMENT D'UN CONSULTANT INDIVIDUEL EN VUE DE L'ELABORATION D'UN PLAN DU CONTINUITE DE L'ACTIVITE ET D'UN PLAN DE REPRISE SUR INCIDENT IT DU FEICOM – EXERCICE 2025

11- ADRESSE DE DEPOT DES CANDIDATURES ET RENSEIGNEMENTS COMPLEMENTAIRES :

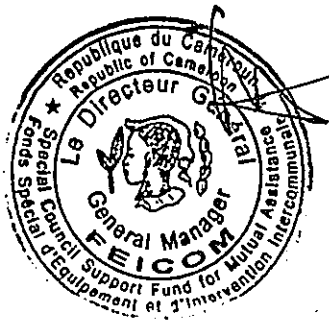
DIRECTION GENERALE DU FEICOM
Service des Marchés et Approvisionnements, Porte 11, Poste 217, sis à l'ancien siège du FEICOM
Quartier Mimboman BP 718 Yaoundé, FEICOM Rue 4.561, Mimboman Yde 4ème
Cameroun
Tel (237) 222 23 51 64- Fax (237) 222 23 17 59

Ampliations :

- MINMAP ;
- ARMP (pour publication et archivage) ;
- AFFICHAGE (pour information) ;
- Chronos/Archives.

Fait à Yaoundé, le 13 A FEV 2025

Le Directeur Général,
Maître d'Ouvrage



Philippe Camille Akoa
MAGISTRAT HORS-HIERARCHIE

REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

FONDS SPECIAL D'EQUIPEMENT ET D'INTERVENTION INTERCOMMUNALE

NOTICE OF SOLICITATION FOR EXPRESSION OF INTEREST N°02/ASMI/FEICOM/DG/2025 OF 14 FEV 2025

FOR THE RECRUITMENT OF AN INDIVIDUAL CONSULTANT FOR THE DEVELOPMENT OF A BUSINESS CONTINUITY PLAN AND AN IT INCIDENT RECOVERY PLAN FOR FEICOM – FINANCIAL YEAR 2025

1-CONTEXT AND JUSTIFICATION

The modernization of the management of the Special Fund for Intercommunal Equipment and Intervention (FEICOM) has been one of the organization's major objectives for several years, hence its inclusion in the various planning documents. Indeed, following several institutional audits, strong recommendations were made to the FEICOM management team in this regard. In order to provide solutions, the company adopted an innovative management approach by implementing Quality and Environmental Management Systems, Management Control, Internal Audit and Risk Approach.

At the level of the Information System (IS), several tools have been deployed singe 2015: the ERP (Enterprise Resources Planning) called Axiome Solution FEICOM (ASOFEI), the interconnection of the General Management with the Regional Agencies, IP telephony, collaborative messaging, etc. In order to guarantee the continuity of activities that are highly dependent on its mainly digitalized Information System, it is becoming urgent for FEICOM to equip itself with a continuity plan for all of its activities (PCA), in order to guarantee the non-interruption of these activities, as they generate value. The Incident Recovery Plan (PRI) that accompanies the first, will allow the organization to define actions for the gradual recovery of IT services, taking into account their criticality and numerous technical and organizational parameters.

In order to achieve this, FEICOM began with a study allowing it to assess the current impact of digitalization on its operations. This approach offers the advantage of giving the organization better visibility into the relationship between business processes and the digital tools that support them. In addition, it identifies different risk scenarios and their impact on the organization in the event of a crisis or disaster. These elements serve as input to the PCA/PRI development process. This preliminary study having been carried out, FEICOM would like to move on to the next stage relating to the development of the tools mentioned above. In this sense, the recruitment of an individual consultant, an expert in the field, to support the organisation in this phase of the project is envisaged.

2. OBJECTIVE OF THE SERVICE

Through the development of a business continuity plan (BCP) and an Incident Recovery Plan (IRP), FEICOM aims to develop a strategy and a set of provisions to ensure the recovery and continuity of its activities following a disaster or an event seriously disrupting its operations. The aim here is to minimize the impact of an IS crisis on the implementation of the organization's missions. This can be translated into the following specific objectives :

- Define a service continuity and recovery strategy, based on the results of the previously conducted business impact study.

- Propose a set of tools and procedures to ensure, in the event of a disaster, the availability of FEICOM's major activities.

- Define the optimal infrastructure and application architectures for the recovery and continuity of services.

- Propose a set of tools and procedures to follow in order to restart the computer system as soon as possible, and with the minimum loss of data, following a disaster.

- Raise awareness and train the various stakeholders on the tools implemented.

- Transfer skills to CSI staff who will have to take over.

3. NATURE AND CONSISTENCY OF THE SERVICES

From an operational point of view, the following results are expected from the implementation of this project.

• Better alignment of the IS with the contextual elements of the organization: by describing the objectives and obligations of the company, from which the list of essential activities to accomplish them will result. This list is accompanied by the various processes necessary for the operation of said activities.

• A methodological and structured approach to responding to the most critical risks: the PCA/PRI makes it possible to identify the most serious risks for the continuity of essential activities, accompanied by several scenarios as to their occurrence.

• Identification of roles and responsibilities in the event of a crisis: the PCA/PRI sets up an organization that identifies the various responsible persons, their role and the procedures for implementing the PCA, accompanied by the associated means to be able to execute it.

• Better crisis management : operationalizing the PCA/PRI makes it possible to define the procedures for incident detection, qualification, escalation, alert, mobilization or even activation of the crisis unit as well as the thresholds for triggering PCA measures and associated communication.

• Operational maintenance of the PCA/PRI keeps the company alert.

At the strategic level, the implementation of a PCA/PRI will contribute to FEICOM's performance in more than one way:

• At the financial level: maintaining financial results, anticipating new expenses induced by crises;

• At the customer relationship level: maintaining the trust of customers and partners, as well as principals and other interested parties;

• At the compliance level: compliance with legal and contractual obligations;

• At the image and responsibility level: the PCA/PRI is proof of good governance that will increase the organization's visibility and maintain trust among stakeholders .

4. METHODOLOGY

The achievement of the objectives mentioned above will be done by implementing specific actions, materialized by the production of deliverables at each stage.

These actions could be presented in three main stages which are the development of the business continuity plan (BCP), the development of the incident recovery plan (IRP) as well as the Training and transfer of skills to the FEICOM personnel indicated.

#	ACTIVITIES	DESCRIPTION	DELIVERABLES
		STEP 1: Business Continuity Plan (BCP)	
1	Appropriation and exploitation of BIA output elements	This will involve analyzing the BIA deliverables, extracting the contextual elements, identifying the risks, identifying the consequences on the activities as well as the measures.	Proposal of the scope of the PCA - Analysis of requirements for interested parties - Mapping of optimized risks - Update of BIA deliverables (Recovery Point Objectives (RPO), Recovery Time Objectives (RTO), etc.)

2	Definition of the business continuity strategy	It allows to formalize the business continuity mechanisms to ensure that the critical activities of the scope can be carried out in the event of a serious incident on the IS.	Listing of risk scenarios to be mitigated, and corresponding response plan - Business continuity strategy in alignment with that of the organization and with the objectives of the business processes.
3	Development of PCA implementation and evaluation tools	It will allow to define a minimum level of service acceptable for the CSI, in order to guarantee the achievement of the objectives of the businesses in the event of a malfunction.	- Procedures and work instructions for continuity - Crisis management procedure (Crisis Committee, Roles and responsibilities of the actors) - Crisis communication plan - IT incident monitoring unit and work instructions - Proposal of tools or technologies adapted to the FEICOM technical environment and to the normative requirements.
STEP 2: Incident Recovery Plan (IRP)			
4	Definition of the Incident Recovery Strategy	It allows to formalize the mechanisms of operation in degraded modes and technical recovery, to identify priorities in advance, to define the level of service to be restored and the associated deadlines. It will also allow the prior identification of the order of priority of recovery and gradual switchover to normal systems (IT site, building, etc.) .	- Listing of identified risk scenarios to be mitigated, and corresponding recovery plan - Business recovery strategy in alignment with that of the organization and with the objectives of the business processes.
5	Development of PRI implementation and evaluation tools	During this activity, technical and organizational tools (equipment, technical architecture, procedure, etc.) must be proposed with a view to optimizing data backup mechanisms, restoration (architecture and equipment, recovery site) and IT incident recovery tests. -	- Optimized backup procedure - Restoration procedure - Recovery test procedure - Technical architectures and recovery tools - Proposal of backup equipment - Proposal of recovery site
Step 3: Training and transfer of skills			
6	Communication and Awareness on the PCA/PRI	- Raising awareness among managers of structures of the concepts of continuity and resumption of activities - Appropriation of focal points of the continuity and resumption plans developed	- Communication and awareness plan - -Awareness and communication materials (flyers, mini videos, etc.) - Training materials.
7	Training and transfer of technical skills	Transfer of skills and training of CSI managers in the assessment and treatment of risks, as well as in the continuity of IT	- Training materials -- Training certificates -

5. CONSULTANT PROFILE

Consultants applying must fulfill the following condition :

- Specialization in the mission:
  - Hold an up-to-date accreditation from the National Agency for Information and Communication Technologies (ANTIC) for IS audits;

- Hold an up-to-date accreditation from certification bodies for the implementation and certification audit of IS to ISO standards in one of the following areas :
  - Information Security Management System ;
  - Business Continuity Management System ;
  - Information Risk Management System.

- Be an expert consultant in the following areas : Information Governance, Risks, Information Security Management, cyber security, cyber investigations and cyber defense strategy

Justify the qualifications listed below:

- Experience in the implementation of IS governance systems: provide proof of at least seven (07) years in the development of strategies, policies, procedures and manuals in the areas of information security and data governance (present supporting documents for projects carried out);
- Experience in ISMS implementation missions: provide proof of at least 03 Information Security Management Systems (ISMS) implementation missions over the last five years;
- Experience in ISMS audit missions: provide proof of at least 03 security audit and cyber risk assessment missions over the last five years;
- Experience in PCA/PRI support or implementation missions: provide proof of at least one implementation mission for the development and/or implementation of a Data Protection and Data Recovery strategy over the last three years;
- Experience in cyber security, cyber defense and cyber investigation missions; provide evidence of having conducted at least three major cyber investigations (for an organization with at least 150 employees) in the last two years;
- Consultant Qualifications

  - Qualifications for the mission (minimum bac +5) in organizational management, information systems management, or any other equivalent diploma (detailed CV, and copies of diplomas, etc.) ; Certifications requises pour la mission, au moins quatre des huit ci-après :

    - An ISO 27001 V2022 certification, Lead auditor,
    - An ISO 27001 V2022 certification, Lead implementer,
    - An ISO 27005 V2018 certification,
    - An EC-Council Incident Handling (ECIH V2) certification,
    - An EC-Council Computer Hacking Forensic Investigator (CHFI) certification,
    - An EDRP V3 certification,
    - A CEH (Ethical Hacking) certification,
    - A CDPO (Certified Data Protection Officer) certification.

6. QUALIFICATION OR EVALUATION CRITERIA

For the Administrative File, the following administrative documents are required :

- A stamped letter of expression of interest;
- A certificate of non-exclusion from public markets issued by the ARMP ;

- A certified copy of the taxpayer card;
- Certified certificate and location plan.

* NB: All tax documents must be dated less than three months ago.

For the Technical File, the following documents must be produced:
Each Consultant will provide:

A technical reference file presenting the documents certifying the consultant's specialization for the mission :
- ANTIC approval;
- Approval for the implementation and audit of certification to the required ISO standards ;
- Expertise in the areas of the mission.

A file of Consultant Experience (Consultant References Qualification and Skills

- Experience in missions to set up IT governance systems: ;
- Experience in ISMS implementation missions ;
- Experience in ISMS audit missions ;
- Experience in missions to support or implement PCA/PRI ;
- Experience in cyber security, cyber defense and cyber investigation missions ;

A file including the consultant's qualifications ;
- Qualifications for the mission (CV, and copies of diplomas, etc.) ;
- Certifications required for the mission (2 points per certification required) ;
- Methodology and understanding of the mission.

7. TECHNICAL FILE EVALUATION CRITERIA

Evaluation criteria	Distribution	Points	
		Number	Subtotal
GENERAL PRESENTATION	Format	1,5 pts	05 pts
	Respect the order of the parts	1,5 pts	
	Dividers	2 pts	
TECHNICAL REFERENCES OF THE CONSULTANT	ANTIC approval;	5 pts	15 pts
	Approval for the implementation and audit of certification to the required ISO standards;	5 pts	
	Expertise in the areas of the mission.	5 pts	
EXPERIENCE OF THE CONSULTANT (References of the Consultant Qualification and Skills Justify the contracts	Experience in missions to set up IT governance systems: 10%;	10	50 pts
	Experience in missions to implement ISMS: 10%;	10	
	Experience in missions to audit ISMS: 10%;	10	
	Experience in missions to support or implement PCA/PRI: 10%;	10	

	Experience in missions involving cyber security, cyber defenses and cyber investigations: 10%.	10	
QUALIFICATIONS OF THE CONSULTANT	Certified diplomas plus signed and dated CV	5	10 pts
	Certifications required for the mission (2 points per certification required)	5	
METHODOLOGY AND PLANNING OF EXECUTION OF SERVICES AND UNDERSTANDING OF THE MISSION	Intervention methodology : *Good (12 pts) *Average (08 pts) *Weak (05 pts)	12 pts	20 pts
	Execution schedule in accordance with the methodology: *Good (04 pts) *Average (2 pts) *Weak (01 Pts)	4 pts	
	*Good understanding (04 pts) *Average understanding (2 pts) *Poor understanding (01 Pts) (at least 3 observations)	4 pts	
TOTAL			100 pts

Only technical offers having obtained 80 points or more will be eligible for examination of financial offers.

8. DURATION OF THE MISSION

This mission must be completed within one hundred and twenty (120) working days. These deadlines are automatically suspended during the validation phases of the deliverables.

Service orders will be notified by the Contract Engineer at the end of each period. The provisional reports will be produced and validated within seven (07) days following receipt and the final report within fourteen (14) days maximum.

9. FINANCING

The services covered by this Notice of Request for Expression of Interest will be financed by the budget of the Special Fund for Equipment and Intercommunal Intervention, Fiscal Year 2025.

10. STATEMENT TO BE ENTERED :

The expression of interest files must be sent in five (05) copies in French or English, in a sealed envelope, to the following address, no later than 10 a.m., with the following statement :

"NOTICE OF SOLICITATION FOR EXPRESSION OF INTEREST N°003/ASMI/FEICOM/CIPM/2025 OF 04 FEV 2025 FOR THE RECRUITMENT OF AN INDIVIDUAL CONSULTANT FOR THE DEVELOPMENT OF A BUSINESS CONTINUITY PLAN AND AN IT INCIDENT RECOVERY PLAN FOR FEICOM – FINANCIAL YEAR 2025

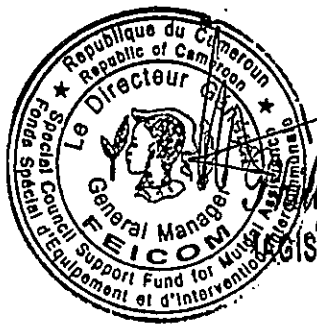
11- ADDRESS FOR SUBMITTING APPLICATIONS AND ADDITIONAL INFORMATION :

The Contracts and Supplies Service, located in the farmer Head Office of FEICOM in Yaounde (Mimboman), P. O. Box 718 Yaounde, FEICOM, Street 4.561, MIMBOMAN YDE IV, Telephone 222 23 51 64 ; Extension 217; Room 11; Fax 222 23 17 59.

Yaounde, the 14 FEV 2025
The General Manager,

Ampliations :

- MINMAP ;
- ARMP (pour publication et archivage) ;
- AFFICHAGE (pour information) ;
- Chronos/Archives.



Philippe Camille Akoa
MAGISTRAT HORS-HIERARCHIE