REPUBLIQUE DU CAMEROUN
Paix - Travail - Patrie

CONSEIL NATIONAL DES CHARGEURS DU CAMEROUN

COMMISSION INTERNE DE PASSATION DES MARCHES

REPUBLIC OF CAMEROON
Peace - Work - Fatherland

CAMEROON NATIONAL SHIPPERS'S COUNCIL

INTERNAL TENDER BOARD

**AVIS DE SOLLICITATION À MANIFESTATION D'INTÉRÊT N°005/ASMI/CNCC S.A/DG/CCGM/CSM/2026 DU 17/04/2026 POUR L'ASSISTANCE SUR LA SECURISATION ET LA PROTECTION DU SYSTEME D'INFORMATION BESC 3.0 DU CONSEIL NATIONAL DES CHARGEURS DU CAMEROUN (CNCC S.A)**

**FINANCEMENT : BUDGET DU CNCC S.A – EXERCICE 2026**

## 1. CONTEXTE

Afin de se conformer aux exigences de l'Etat en matière de sécurité des systèmes d'information, le CNCC S.A sollicite l'assistance d'un cabinet externe pour l'accompagner dans cette démarche au travers de la sécurisation et la protection de son système d'information. Cette prestation permettra de mener une évaluation approfondie dont les objectifs seront de :

- Ressortir l'état du système d'information en toute objectivité et indépendance dans le respect des clauses de confidentialité et de non divulgation ;
- Analyser des risques qui pèsent sur le CNCC S.A ;
- Déceler les failles de sécurité et proposer des solutions correctives à court, moyen et long terme ;
- Evaluer la robustesse des moyens de protection mis en place pour sécuriser le système d'information.
- Etablir des scénarii de réduction des risques ;
- Proposer un plan de mise en œuvre des recommandations dont l'objectif est de permettre au CNCC S.A d'être résilient aux risques de sécurité de toute nature ;
- Mettre en œuvre les jalons d'un système de contrôle interne efficace et performant intégrant toutes les autres fonctions d'assurance.
- L'analyse et la cartographie des risques pesant sur la continuité de ses activités ;
- L'élaboration d'un Plan de Continuité d'Activité (PCA) définissant les modalités de fonctionnement en mode dégradé lors d'une crise ;
- L'élaboration d'un Plan de Reprise d'Activités (PRA) fixant les procédures de rétablissement des systèmes, processus et services critiques après un sinistre ;
- La mise en place d'un cadre de gouvernance assurant la pérennité et la révision périodique de ces plans.

## 2. OBJET

L'objectif général de la présente mission est d'effectuer l'audit du système d'information BESC 3.0 du CNCC S.A d'une part et de doter le CNCC S.A d'un cadre documenté, opérationnel et éprouvé de continuité et de reprise d'activités, permettant à l'institution de faire face à tout événement perturbateur majeur tout en maintenant un niveau de service acceptable pour l'ensemble de ses parties prenantes, d'autre part.

## 3. CONSISTANCE DES TRAVAUX

La présente mission s'articulera autour de deux (02) phases principales, à savoir :

***Phase 1 : L'AUDIT DE SECURITE DU SYSTEME D'INFORMATION BESC 3.0***

- D'Identifier les forces et les faiblesses du Système d'Information du CNCC S.A ;
- De poser un diagnostic et une analyse des risques de sécurité Système d'Information du CNCC S.A ;
- De proposer des recommandations permettant de traiter les risques identifiés et d'optimiser la sécurité du Système d'Information du CNCC S.A.

**Livrables**

Les livrables de la mission d'audit de sécurité du système d'information du CNCC S.A sont :

- **Livrable 1 :** Le Rapport d'audit de sécurité Système d'Information du CNCC ;
- **Livrable 2 :** Le Plan de Mise en œuvre des recommandations de l'audit de sécurité.

***Phase 2 : PLAN DE REPRISE D'ACTIVITES (PRA) ET PLAN DE CONTINUITE D'ACTIVITE (PCA)***

**a) Diagnostic et état des lieux**

- ✓ Revue documentaire (politiques, procédures, chartes existantes, contrats fournisseurs, plans d'urgence) ;
- ✓ Entretiens avec les responsables de chaque Direction et les correspondants techniques ;
- ✓ Inventaire des ressources critiques (systèmes, données, compétences, locaux, équipements) ;
- ✓ Évaluation du niveau de maturité du CNCC S.A en matière de continuité et de résilience.

**b) Analyse des risques et des impacts (BIA & Risk Assessment)**

- ✓ Identification et cartographie des risques (techniques, organisationnels, humains, environnementaux) ;
- ✓ Réalisation du Bilan d'Impact sur les Activités (BIA) : identification des processus critiques, des dépendances et des ressources minimales requises ;
- ✓ Détermination des DMIA (Durée Maximale d'Interruption Admissible), ODR (Objectif de Délai de Reprise) et RPO (Recovery Point Objective) pour chaque processus critique ;
- ✓ Hiérarchisation des risques selon leur probabilité d'occurrence et leur impact.

### c) Élaboration du Plan de Continuité d'Activité (PCA)

- ✓ Définition des stratégies de continuité pour chaque processus critique ;
- ✓ Description des procédures de fonctionnement en mode dégradé ;
- ✓ Identification et organisation de la cellule de crise (rôles, responsabilités, suppléances) ;
- ✓ Définition des procédures de communication interne et externe en situation de crise ;
- ✓ Élaboration des fiches réflexes par scénario de crise ;
- ✓ Intégration des exigences légales, réglementaires et contractuelles applicables.

### d) Élaboration du Plan de Reprise d'Activités (PRA)

- ✓ Définition des stratégies de reprise des systèmes d'information et des infrastructures ;
- ✓ Description des procédures de sauvegarde, de restauration et de repli (site de secours) ;
- ✓ Élaboration des procédures de reprise pour chaque système et processus critique ;
- ✓ Définition des séquences de priorité de reprise ;
- ✓ Intégration des configurations techniques et des prérequis de reprise ;
- ✓ Articulation du PRA avec le PCA.

### e) Test, formation et transfert de compétences

- ✓ Conception d'un programme de tests et d'exercices (tests de basculement, simulations de crise, exercices sur table) ;
- ✓ Réalisation d'au moins un exercice de simulation avec les équipes du CNCC ;
- ✓ Formation des responsables de la cellule de crise et des correspondants PCA/PRA ;
- ✓ Élaboration d'un programme de révision périodique et de maintien en condition opérationnelle des plans.

## Livrables

| N° | Livrable | Contenu principal |
|---|---|---|
| L3 | Rapport de diagnostic et d'état des lieux | Inventaire des ressources, niveau de maturité, gaps identifiés |
| L4 | Rapport BIA et analyse des risques | Cartographie des risques, DMIA, ODR, RPO par processus critique |
| L5 | Plan de Continuité d'Activité (PCA) | Stratégies de continuité, fiches réflexes, procédures de crise, organigramme de crise |
| L6 | Plan de Reprise d'Activités (PRA | Procédures de reprise SI, séquences de priorité, configurations de secours |
| L7 | Programme de tests et d'exercice | Planning, scénarios, indicateurs de performance des plans |
| L8 | Rapport de formation et de transfert | Supports de formation, compte-rendu des sessions, recommandations |
| L9 | Rapport de synthèse final | Synthèse exécutive, bilan de la mission, feuille de route de maintien en condition |

### *Méthodologies à mettre en œuvre*

- PCI DSS V3 ;
- ISO 20000 ;
- ISO 22301 : Système de management de la continuité d'activité – exigences ;
- ISO 22313 : Lignes directrices pour la mise en œuvre de la continuité d'activité ;
- ISO 22317 : Lignes directrices pour le Bilan d'Impact sur les Activités (BIA) ;
- ISO 22320 : Management de la sécurité – Gestion des urgences.
- ISO/IEC 27001 : Système de management de la sécurité de l'information ;
- ISO/IEC 27002 : Bonnes pratiques pour la sécurité de l'information ;
- ISO/IEC 27005 : Gestion des risques liés à la sécurité de l'information ;
- COBIT 5 / COBIT 2019 : gouvernance et management des systèmes d'information ;
- EBIOS Risk Manager : méthode d'analyse des risques de l'ANSSI ;
- MEHARI : méthode harmonisée d'analyse des risques ;
- FAIR (Factor Analysis of Information Risk) : quantification des risques ;
- ITAF : cadre de référence pour l'audit des systèmes d'information.
- Owasp Testing Guide ;
- Le « Référentiel d'audit de sécurité des systèmes d'information » de l'ANTIC ;
- Loi N°2010/012 relative à la cyber sécurité et à la cybercriminalité au Cameroun ;
- Loi N°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun ;
- Décret N°2012/1643/PM du 14 Juin 2012 ;
- Outil pour les audits techniques
- Owasp;
- Wireshark ;
- Nmap ;
- Nessus ;
- Netsparker ;
- Network security auditor ;
- Textes réglementaires régissant le CNCC S.A.

## 4. PARTICIPATION ET ORIGINE

La participation au présent Avis de Sollicitation à Manifestation d'Intérêt est ouverte aux entreprises de droit camerounais installées au Cameroun et justifiant des capacités, compétences et expertise avérées dans le domaine.

## 5. FINANCEMENT

L'audit objet du présent Avis de Sollicitation à Manifestation d'Intérêt est financé entièrement par le budget du Conseil National des Chargeurs du Cameroun (CNCC S.A), exercice 2026.

## 6. REMISE DES OFFRES

Les offres rédigées en français ou en anglais en quatre (04) exemplaires, dont un (01) original et trois (03) copies marquées comme telles, seront déposées à la Direction Générale du Conseil National des Chargeurs du Cameroun (CNCC S.A), au plus tard le 18/05/2026 **à 13h00**, et devront porter la mention :

**AVIS DE SOLLICITATION À MANIFESTATION D'INTÉRÊT N°005/ASMI/CNCC S.A/DG/CCGM/CSM/2026 DU _____ POUR L'ASSISTANCE SUR LA SECURISATION ET LA PROTECTION DU SYSTEME D'INFORMATION BESC 3.0 DU CONSEIL NATIONAL DES CHARGEURS DU CAMEROUN (CNCC S.A)**

***« A N'OUVRIR QU'EN SEANCE DE DEPOUILLEMENT »***

## 7. COMPOSITION DU DOSSIER

**a) Pièces administratives :**

- Une lettre de motivation timbrée et dûment signée par le candidat ;
- L'attestation de non faillite délivrée par le greffe du TPI du domicile;
- L'attestation de conformité fiscale timbrée et datant de moins de trois (03) mois;
- Le certificat de non exclusion de l'ARMP relatif à l'Avis de Sollicitation à Manifestation d'Intérêt N°005/ASMI/CNCC S.A/DG/CIPM/2026 du _____ pour l'audit du système d'information du CNCC S.A;
- L'attestation d'immatriculation accompagnée d'un plan de localisation signé sur l'honneur.

**b) Dossier technique :**

- **Références du cabinet**

➢ Expérience générale sur des projets exécutés dans le management de la sécurité des systèmes d'informations (élaboration des politiques de sécurité des SI, réalisation des audits de sécurité des SI, renforcement des capacités en sécurité des systèmes d'information) au cours des cinq (05) dernières années (2021, 2022, 2023, 2024 et 2025) à justifier par quatre (04) contrats enregistrés (1ere et dernière page, PV de réception) ;

➢ Expérience spécifique sur les projets exécutés sur l'audit des systèmes d'information avec une entité publique ou parapublique au cours des cinq(05) dernières années (2021, 2022, 2023, 2024 et 2025) à justifier par au moins un (01) contrat enregistré (1er et dernière page, PV de réception).

- **Qualification du personnel :**

➢ ***Un (01)* ingénieur de conception *chef de mission***

- Diplôme: BACC+5 au moins en sécurité des systèmes d'information (justifié par la photocopie certifiée du diplôme).
- Au moins deux certifications parmi les suivantes : Project Management Professional (PMP), CISM, ISO2700X, CEH, CISA ou une certification en forensique et investigation. Justifié par la photocopie certifiée de la certification.
- Expérience : Avoir dirigé en tant que chef de projet au moins deux (02) projets dans le management de la sécurité des SI (Elaboration des politiques de sécurité des SI, réalisation des audits de sécurité des SI, ou investigations numériques) avec une administration publique ou parapublique à justifier dans un CV signé et daté
- Années d'expérience : Au moins quinze (15) ans d'expérience dans la conduite des opérations d'audit des systèmes d'information, à justifier dans un CV signé et daté.

➢ ***Un (01) Expert en Sécurité Informatique***

- Diplôme: BACC+5 au moins en informatique/télécommunication (justifié par la photocopie certifiée conforme du diplôme) ;
- Certification : Certification CISM ou CISA, Justifié par la photocopie certifiée de la certification ou l'attestation de présentation de l'original de la certification.
- Expérience : Au moins deux (02) participations dans des projets de management de la sécurité des Systèmes d'Information (élaboration des politiques de sécurité des Systèmes d'Information, réalisation des audits de sécurité des Systèmes d'Information, ou tout autre projet en sécurité des Systèmes d'Information) avec des entités publiques ou parapubliques, à justifier dans un CV signé et daté
- Années d'expérience : Dix (10) ans d'expérience au moins en sécurité des Systèmes d'Information, à justifier dans un CV signé et daté

➢ ***Un (01) Expert en sécurité des systèmes d'information***

- Diplôme: BACC+5 au moins en informatique ou télécoms (justifié par la photocopie certifiée conforme du diplôme) ;
- Certification : Certifié ISO2700X, CISA, CISM, Certified Ethical Hacking (CEH) ou CCNA Security, Justifié par la photocopie certifiée de la certification.
- Expérience : Au moins une (01) participation dans un projet gouvernemental de politique de sécurité ou de stratégie de sécurité., à justifier dans un CV signé et daté.
- Années d'expérience : Dix (10) ans d'expérience au moins en sécurité informatique, à justifier dans un CV signé et daté.

- **Compréhension du travail et méthodologie proposées**
  - ➢ Compréhension du travail demandé
  - ➢ Méthodologie de travail et planning de réalisation

## 8. CRITERES D'EVALUATION

### a) Critères éliminatoires

Les critères éliminatoires sont les suivants :

- Offre administrative incomplète au terme d'un délai éventuel accordé ;
- Fausse déclaration ou pièces falsifiées ;
- Absence de justificatif d'au moins une expérience dans les prestations exigées dans la grille d'évaluation ;
- Note de qualification inférieure à 80 points sur 100
- Absence de l'agrément de l'ANTIC.

### b) Critères essentiels

Les critères essentiels sont les suivants :

**1- Compréhension du travail et méthodologie proposées (20 points)**
**2- Références du cabinet (50 points)**
**3- Personnel du Cabinet (25 points)**
**4- Présentation générale de l'offre (05 points)**

## GRILLE DE NOTATION

| N° | CRITERES D'EVALUATION | NOTATION |
|---|---|---|
| 1 | **Compréhension du travail et méthodologie proposées** | **20 Points** |
| | Compréhension du travail demandé | **10 Points** |
| | Méthodologie de travail et planning de réalisation | **10 Points** |
| 2 | **Références du Cabinet** | **50 Points** |
| a | Expérience générale sur des projets exécutés au cours des cinq (05) dernières années (2021, 2022, 2023, 2024 et 2025) à justifier par 4 contrats enregistrés (1er et dernière page, et PV de réception) ; 10 points par contrat justifié. | 40 Points |
| b | Expérience spécifique sur un projet **dans le management de la sécurité des SI (élaboration des politiques de sécurité des SI, réalisation des audits de sécurité des SI, renforcement des capacités en sécurité des systèmes d'information** avec une entité publique au cours des cinq (05) dernières années (2021, 2022, 2023, 2024 et 2025) à justifier par 1 contrat enregistré (1er et dernière page, et PV de réception); 10 points pour le contrat justifié.<br>NB : Le projet spécifique justifié ne doit pas être parmi ceux cités dans l'expérience générale. | 10 Points |
| 3 | **Personnel du Cabinet** | **25 Points** |
| a | **Un (01) ingénieur de conception chef de mission** | ***10 Points*** |
| a1 | Diplôme: BACC+5 au moins en sécurité des systèmes d'information B (justifié par la photocopie certifiée du diplôme) | 2 Points |
| a2 | Justificatifs de l'expérience : Au moins deux (02) participations à justifier en qualité de chef de mission dans des projets similaires. Joindre le CV signé et daté (02 points par justificatif) | 4 Points |
| | Au moins deux certifications parmi les suivantes: Project Management Professional (PMP), CISM, ISO2700X, CEH ,CISA ou une certification en forensique et investigation (Justifié par la photocopie certifiée de la certification). | 2 points |
| a3 | Au moins quinze (15) ans d'expérience dans la conduite des opérations d'audit des systèmes d'information. Joindre le CV signé et daté. | 2 Points |
| b | **Un (01) Expert en sécurité informatique** | ***10 Points*** |
| b1 | Diplôme : BACC+5 au moins en informatique/télécommunication, (justifié par la photocopie certifiée du diplôme) | 2 Points |
| b2 | Justificatifs de l'expérience : Au moins deux (02) participations à justifier dans des projets similaires. Joindre le CV signé et daté (2 points | 4 Points |

| | | |
|---|---|---|
| | par justificatif) | |
| | Certification CISM ou CISA (Justifié par la photocopie certifiée de la certification). | 2 Points |
| **b3** | Au moins dix (10) ans d'expérience professionnelle dans la sécurité des systèmes informatiques. Joindre le CV signé et daté. | 2 Points |
| **c** | **Un (01) Expert en sécurité des systèmes d'information** | ***05 Points*** |
| **c1** | Diplôme: BACC+5 en informatique ou télécommunications (justifié par la photocopie certifiée du diplôme) | 2 Points |
| **c2** | Certifié ISO2700X, CISA, CISM, Certified Ethical Hacking (CEH) ou CCNA Security | 2 Points |
| **c3** | Au moins dix(10) ans d'expérience en sécurité informatique. Joindre le CV daté et signé. | 1 Points |
| **4** | **Présentation générale de l'offre** | **5 Points** |
| **a** | Présentation bonne (clarté, lisibilité, table de matière, pagination, qualité des pièces jointes) | 5 Point |
| **b** | Présentation moyenne (absence d'une des qualités citées) | 3 Point |
| **c** | Présentation mauvaise (absence d'au moins deux des qualités citées) | 1 Point |
| | **TOTAL** | **100 Points** |

## 9. RENSEIGNEMENTS COMPLÉMENTAIRES :

Les renseignements complémentaires peuvent être obtenus aux heures ouvrables au Secrétariat du Directeur Général du Conseil National des Chargeurs du Cameroun (CNCC S.A) à Douala, au Centre des Affaires Maritimes, 3ème étage Immeuble IGH. Tél. : 233 43 67 67 Fax : 233 43 70 17, dès publication du présent avis.

**Douala, le** 17/04/2026

**Le Directeur Général**

CONSEIL NATIONAL DES CHARGEURS DU CAMEROUN – Le Directeur Général – NATIONAL SHIPPER'S COUNCIL

***Auguste MBAPPE PENDA***

**Ampliations** :
- JDM/ARMP
- CIPM/CNCC S.A
- ARCHIVES
- AFFICHAGE