Réf. : ECW/BAG/ADM/06-26-103/oja **Date : 29 July 2026**

APPEL À PROPOSITIONS

PRESTATION DE SERVICES D'AUDIT DES SYSTÈMES D'INFORMATION (SI)

Le Bureau de l'Auditeur Général des institutions de la CEDEAO (BAG) invite par la présente les cabinets d'audit qualifiés et expérimentés à soumettre des offres techniques et financières pour la prestation de services d'audit des systèmes d'information (SI) dans le cadre d'un accord-cadre d'une durée de trois ans.

Cette mission vise à aider le Bureau de l'Auditeur Général à mener des audits des systèmes d'information fondés sur les risques dans l'ensemble des institutions, agences et bureaux de la CEDEAO. Les services couvriront des domaines tels que la gouvernance des TIC, la cybersécurité, la gestion des risques, la sécurité de l'information, la gouvernance des données, la continuité des activités et la reprise après sinistre, les applications professionnelles, la conformité réglementaire et d'autres activités connexes d'audit des systèmes d'information.

AVIS IMPORTANT

Il est vivement recommandé aux cabinets intéressés d'examiner attentivement le cahier des charges (CdC) ci-joint avant de préparer et de soumettre leurs offres. Le cahier des charges fait partie intégrante du présent appel d'offres et contient des informations détaillées concernant l'étendue des services, les conditions d'éligibilité, les qualifications requises des consultants, les critères d'évaluation technique, la méthodologie, les livrables, les modalités d'établissement de rapports, les conditions de paiement et les obligations contractuelles.

La soumission d'une offre vaut confirmation que le soumissionnaire a pris connaissance, compris et accepté les exigences et conditions énoncées dans le cahier des charges.

ÉLIGIBILITÉ

Les cabinets éligibles doivent justifier d'une expérience significative en matière d'audit des systèmes d'information et posséder l'expertise technique, les certifications professionnelles et les ressources nécessaires pour mener à bien des missions de cette nature, comme détaillé dans le cahier des charges ci-joint.

EXIGENCES RELATIVES À LA SOUMISSION

Les cabinets intéressés doivent soumettre les éléments suivants :

- une offre technique ;
- une offre financière ;
- un profil du cabinet ;
- des justificatifs d'expérience pertinente ; et
- des documents justificatifs d'éligibilité et des certifications tels que spécifiés dans le cahier des charges.

MODALITÉS DE SOUMISSION D'OFFRES ET DATE LIMITE

Les offres peuvent être soumises par voie électronique ou remises sur support papier à l'adresse indiquée ci-dessous :

Soumission d'offres par voie électronique : BAG-procurement-lcb@ecowas.int

Soumission d'offres sur support papier : Bureau de l'Auditeur Général des institutions de la CEDEAO, 10 Dar es Salam Crescent, Wuse 2, Abuja, Nigéria.

Date limite : toutes les offres doivent être reçues au plus tard le 29 Août 2026.

INSTRUCTIONS IMPORTANTES

- Les offres soumises par voie électronique doivent porter l'objet suivant : **« Offre relative à la prestation de services d'audit des systèmes d'information (SI) – Réf. : ECW/BAG/ADM/06-26-103/oja ».**
- Les soumissionnaires s'assurent que leurs offres répondent pleinement à l'ensemble des exigences énoncées dans le cahier des charges ci-joint.
- Le manquement à fournir les informations, les qualifications, les pièces justificatives ou les certifications requises dans le cahier des charges peut entraîner la déclaration de non-conformité de l'offre.
- Les soumissions d'offres tardives ne seront pas prises en considération.

- Le Bureau de l'Auditeur Général se réserve le droit d'accepter ou de rejeter toute offre et n'est pas tenu de procéder à une adjudication suite au présent appel d'offres.
- La publication de cet appel à propositions ne constitue pas un engagement de la part du Bureau de l'Auditeur Général d'attribuer un marché ou de rembourser quelque frais engagé pour la préparation et la soumission d'offres.

DEMANDES D'ÉCLAIRCISSEMENTS

Toute demande d'éclaircissements concernant le présent processus de passation de marché doit être soumise par écrit à :
BAG-is-procurement@ecowas.int

BUREAU DE L'AUDITEUR GÉNÉRAL DES INSTITUTIONS DE LA CEDEAO (BAG)

CAHIER DES CHARGES (CdC)

PRESTATION DE SERVICES D'AUDIT DES SYSTÈMES D'INFORMATION (SI)

TABLE DES MATIÈRES

APPEL À PROPOSITIONS 1

PRESTATION DE SERVICES D'AUDIT DES SYSTÈMES D'INFORMATION (SI) 1

AVIS IMPORTANT 1

ÉLIGIBILITÉ 2

EXIGENCES RELATIVES À LA SOUMISSION 2

MODALITÉS DE SOUMISSION D'OFFRES ET DATE LIMITE 2

INSTRUCTIONS IMPORTANTES 2

DEMANDES D'ÉCLAIRCISSEMENTS 3

1. CONTEXTE ET CADRE 6

2. OBJECTIFS DE LA MISSION 7

3. ÉTENDUE DES SERVICES 7

Les cabinets d'audit des systèmes d'information sélectionnés entreprendront des missions annuelles d'audit des systèmes d'information fondées sur les risques, qui couvriront, sans s'y limiter, les domaines ci-après. 7

4. MÉTHODOLOGIE ET APPROCHE 10

5. LIVRABLES 11

6. MODALITÉS D'ÉTABLISSEMENTS DE RAPPORTS 11

7. QUALIFICATIONS DES CABINETS ET COMPOSITION DE LEUR ÉQUIPE 11

8. NORMES PROFESSIONNELLES 13

9. CONFIDENTIALITÉ ET PROTECTION DES DONNÉES 14

10. TRANSFERT DE CONNAISSANCES ET RENFORCEMENT DES CAPACITÉS 15

11. INDICATEURS CLÉS DE PERFORMANCE (ICP) 16

13. DURÉE DE LA MISSION 17

1. CONTEXTE ET CADRE

Au cœur de la Vision 2050 de la CEDEAO se trouve une communauté de citoyens intégrée dans une région paisible et prospère, dotée d'institutions solides qui respectent les libertés fondamentales et œuvrent à un développement inclusif et durable. À cet égard, le Président de la Commission de la CEDEAO est chargé de mobiliser les citoyens de la région autour de cette vision et de contribuer à sa réalisation à l'horizon 2050.

Le Bureau de l'Auditeur Général (BAG) a été créé en 2018 par la Conférence des Chefs d'État et de gouvernement, après un processus de réforme institutionnelle, en tant qu'institution de contrôle indépendante. Dans le cadre de l'engagement visant à améliorer le processus d'intégration de l'Afrique de l'Ouest tout en renforçant son efficacité, le Bureau de l'Auditeur Général est chargé de garantir la transparence et la responsabilité de l'ensemble des institutions, agences et bureaux de la CEDEAO.

Après l'approbation d'un plan stratégique, le Bureau de l'Auditeur Général entend conclure un contrat-cadre d'une durée de trois ans avec un cabinet d'audit afin de l'assister dans les audits des institutions, agences et bureaux de la CEDEAO, lesquels audits comprennent notamment des examens des systèmes informatiques. Le Bureau de l'Auditeur Général entend affecter une partie de ses dotations budgétaires annuelles à la conclusion d'un accord-cadre avec un cabinet indépendant pour lui fournir des services d'audit des systèmes d'information (SI) dans le cadre d'un appel d'offres régional ouvert et concurrentiel pour la prochaine période triennale courant à compter de juin 2026.

L'objectif de cette mission est de garantir que l'environnement TIC de la CEDEAO reste sécurisé, résilient, bien gouverné et pleinement conforme aux normes, cadres et exigences réglementaires internationalement reconnus applicables à la CEDEAO. Par conséquent, sous la supervision du Bureau de l'Auditeur Général (BAG), le cabinet d'audit des systèmes d'information désigné collaborera avec le BAG, dont le siège se trouve à Abuja, au Nigéria, afin d'évaluer et de renforcer la gouvernance informatique, la situation en matière de cybersécurité, les systèmes de contrôle interne et les processus de gestion des risques opérationnels de l'ensemble des institutions, agences et bureaux de la CEDEAO.

La présente mission, ainsi que les obligations contractuelles en découlant, seront régies par le Code des marchés de 2021 et le Règlement financier de la CEDEAO de 2021. Partant, l'ensemble des processus de passation de marchés, d'exécution et d'établissement de rapports est soumis au respect rigoureux des principes fondamentaux régissant la commande publique, à savoir la mise en concurrence, la transparence, la responsabilité et l'égalité de traitement.

2. OBJECTIFS DE LA MISSION

Les objectifs de la mission d'audit des systèmes d'information consistent à fournir une assurance indépendante, objective et fondée sur des données probantes quant à l'adéquation, à l'efficacité et à la maturité de la gouvernance des TIC, de la gestion des risques, de la cybersécurité et des environnements de contrôle.

Plus précisément, la mission vise à :

évaluer si les cadres de gouvernance des TIC existants — y compris les structures, les politiques, les processus et les mécanismes de surveillance — fonctionnent efficacement et contribuent à la réalisation de la mission de l'institution ;

identifier les vulnérabilités systémiques, les défaillances des contrôles, les risques liés à la cybersécurité, les lacunes en matière de conformité et les inefficacités des processus susceptibles d'avoir un impact sur la performance ou la résilience de l'organisation ;

procéder à une analyse comparative des pratiques, processus et contrôles informatiques actuels par rapport aux normes et référentiels internationaux établis, tels que COBIT 2019, les normes ISO/IEC 27001 et 27002, le cadre de cybersécurité du NIST, ITIL 4 et les lignes directrices ISSAI applicables ;

formuler des recommandations concrètes, hiérarchisées et fondées sur les risques afin de renforcer la résilience des TIC, d'améliorer la maturité des contrôles et d'accroître l'efficacité et la fiabilité opérationnelles ;

soutenir les instances de contrôle et la haute direction dans le renforcement de la responsabilité, de la transparence et de la pérennité des performances à long terme au dans l'environnement des TIC ; et

promouvoir et préserver la confidentialité, l'intégrité, la disponibilité et la fiabilité globale des actifs d'information, des plateformes numériques et des systèmes professionnels de la CEDEAO.

3. ÉTENDUE DES SERVICES

Les cabinets d'audit des systèmes d'information sélectionnés entreprendront des missions annuelles d'audit des systèmes d'information fondées sur les risques, qui couvriront, sans s'y limiter, les domaines ci-après.

a. Gouvernance informatique et alignement stratégique :

Évaluer l'adéquation et l'efficacité des cadres de gouvernance des TIC, des structures décisionnelles, des mécanismes de pilotage, des instruments politiques, des dispositifs de responsabilisation, ainsi que l'alignement des stratégies, architectures et investissements en matière de TIC sur la mission institutionnelle et les objectifs opérationnels.

b. Gestion des risques liés aux TIC :
Évaluer les méthodologies d'identification des risques, les processus d'évaluation, les critères de hiérarchisation, les pratiques d'atténuation et de suivi, ainsi que l'exhaustivité et la qualité des registres des risques liés aux TIC. S'assurer que les mesures de traitement des risques sont appropriées et proportionnées aux niveaux d'exposition.

c. Gestion de la sécurité de l'information :
Évaluer la conception et l'efficacité opérationnelle des politiques, procédures et dispositifs de contrôle visant à préserver la confidentialité, l'intégrité et la disponibilité des actifs informationnels. Ce volet d'action comprend, notamment, la gestion des identités et des accès, le renforcement des configurations, la journalisation et la surveillance des systèmes, les référentiels de sécurité et les processus de correction des vulnérabilités.

d. Évaluation de la posture en matière de cybersécurité :
Évaluer l'adéquation des contrôles de sécurité du réseau, des plateformes et des terminaux, y compris les défenses périmétriques, les configurations des pare-feu et des systèmes de détection/prévention d'intrusions (IDS/IPS), les capacités de détection et de réponse aux incidents au niveau des terminaux, la gestion des correctifs et des mises à jour, les mesures de protection physiques, ainsi que les processus de détection, de réponse et d'escalade des incidents, conformément aux principes du cadre de cybersécurité du NIST.

e. Gestion des services informatiques (ITSM) :
Examiner les processus opérationnels informatiques tels que la gestion des incidents et des problèmes, la gestion des changements et des mises en production, la gestion des configurations et des actifs, les opérations du centre de services, les dispositions relatives à la continuité des services et la surveillance des performances au niveau des services, conformément aux meilleures pratiques ITIL 4.

f. Gouvernance, protection et confidentialité des données :
Évaluer les contrôles relatifs au cycle de vie des données — notamment la création, la classification, le stockage, la transmission, l'archivage, la conservation et l'élimination — ainsi que la qualité des données, les structures de gestion, la reddition de comptes en matière de gouvernance et la conformité aux exigences régionales et internationales applicables en matière de protection des données.

g. Continuité des activités et reprise après sinistre (BCP/DR) :
Examiner les plans de continuité, les architectures de reprise après sinistre, les stratégies de sauvegarde, les définitions des objectifs de point de reprise/de délai de reprise (RTO/RPO), les dispositions de stockage hors site, ainsi que les preuves attestant de la réalisation de tests périodiques, d'exercices de restauration et d'évaluations de l'état de préparation.

h. Projets informatiques, initiatives numériques et gestion du changement :
Évaluer les dispositifs de gouvernance relatifs au développement des systèmes, aux achats, à la mise en œuvre, à la migration, aux changements de configuration et aux revues post-mise en œuvre. Vérifier l'existence d'une séparation appropriée des tâches, de contrôles de l'environnement et de mécanismes d'implication des parties prenantes.

i. Applications et plateformes professionnelles :
Auditer les contrôles informatiques généraux (GITC) et les contrôles au niveau des applications pour les systèmes professionnelles critiques — notamment SAP ERP, les systèmes de gestion financière, les plateformes de RH et les applications spécialisées — en couvrant les droits d'accès, les contrôles configurables, la journalisation des audits, l'intégrité des données et les mécanismes de contrôle des changements.

j. Examens de conformité des TIC :
Évaluer la conformité aux politiques et procédures internes en matière de TIC, aux obligations réglementaires, aux accords de licence et aux exigences externes applicables au fonctionnement des TIC, y compris les directives des donateurs et les mandats régionaux.

k. Gouvernance de l'IA et alignement stratégique :
Mener des missions d'audit de l'IA fondées sur les risques afin d'évaluer la conception et l'efficacité des cadres de gouvernance de l'IA, des structures de supervision et d'examen éthique, de l'attribution des pouvoirs de décision, des mécanismes de responsabilisation, ainsi que des politiques régissant le développement, l'acquisition, le déploiement, le suivi et la gestion du cycle de vie de l'IA. Évaluer l'alignement de la stratégie en matière d'IA, de la planification des investissements, de l'utilisation des données et des initiatives d'innovation sur les objectifs institutionnels, les exigences réglementaires, les normes éthiques et les principes de gestion des risques opérationnels, afin de favoriser une adoption responsable de l'IA et créatrice de valeur.

l. Conformité réglementaire et politique :
Vérifier le respect des exigences légales, réglementaires et politiques applicables — y compris les règles financières régionales, les conditions de conformité imposées par les donateurs, les lois sur la propriété intellectuelle, les conditions de licence des technologies et les obligations d'utilisation des logiciels libres — dans la mesure où elles concernent le fonctionnement des TIC et la prestation de services.

m. Examens spécialisés et ponctuels :
Réaliser des examens ciblés, des analyses post-incident et des audits des technologies émergentes sur la base de demandes spécifiques formulées par le Bureau de l'Auditeur Général (BAG).

n. Autres domaines d'intervention :
Réaliser des examens spécialisés, thématiques ou ponctuels selon les demandes, tels que des audits d'incidents de cybersécurité, de déploiements de nouvelles technologies, de domaines de risques émergents ou des évaluations de suivi des recommandations d'audit antérieures.

Le champ d'application des services s'étend à l'ensemble des institutions, agences et bureaux de terrain de la CEDEAO relevant du cadre institutionnel de la CEDEAO.

4. MÉTHODOLOGIE ET APPROCHE

L'auditeur appliquera une méthodologie d'audit structurée, fondée sur les risques et étayée par des données factuelles, conforme aux normes ISACA IS Audit & Assurance Standards et à d'autres cadres d'évaluation reconnus au niveau international. L'approche englobera la planification initiale, l'analyse globale des risques, l'élaboration de programmes d'audit détaillés, le travail sur le terrain et les tests techniques, la classification des constatations par niveau de risque (par exemple : critique/élevé/modéré/faible), la préparation des rapports préliminaires et finaux, ainsi que des examens de suivi systématiques visant à évaluer la mise en œuvre des recommandations.

La méthodologie inclut :

a) une planification exhaustive et une évaluation des risques en concertation avec les principales parties prenantes ;
b) l'élaboration de programmes d'audit détaillés et de critères de contrôle ;
c) un travail sur le terrain comprenant des entretiens, des visites sur place, l'examen de la documentation, des échantillonnages, des analyses et des tests techniques, le cas échéant ;
d) la tenue de documents de travail d'audit traçables et vérifiables corroborant les conclusions ;
e) une notation des risques liés aux constats en fonction de leur impact et de leur probabilité ;
f) des discussions de validation avec la direction afin de confirmer l'exactitude des faits ;
g) la rédaction de projets de rapports d'audit structurés et de rapports d'audit finaux ; et
h) des activités de suivi visant à évaluer l'état d'avancement de la mise en œuvre des mesures correctives convenues.

L'approche doit mettre l'accent sur le scepticisme professionnel, l'indépendance, l'objectivité et l'assurance qualité tout au long du cycle d'audit.

5. LIVRABLES

L'auditeur produit les livrables techniques suivants :

a) un plan annuel d'audit des systèmes d'information fondé sur les risques, décrivant les missions, les domaines prioritaires et les échéances indicatives ;
b) des programmes de travail d'audit au niveau de la mission décrivant les objectifs, les critères et les procédures ;
c) des rapports d'étape périodiques résumant l'état d'avancement, les enjeux clés et les risques émergents ;
d) des rapports préliminaires d'audit des systèmes d'information comprenant un résumé, le contexte, le périmètre, la méthodologie, les constatations détaillées, les notations de risque et les recommandations ;
e) des rapports finaux d'audit des systèmes d'information intégrant les réponses de la direction et les plans d'action convenus ;
f) des séances de présentation et d'information destinées au BAG et aux parties prenantes concernées ; et
g) des documents de travail électroniques complets et une documentation justificative suffisante pour permettre l'examen et la conservation par le Bureau de l'Auditeur Général (BAG).

Tous les livrables doivent être clairs, structurés, fondés sur des données factuelles et conformes aux normes professionnelles d'établissements de rapports.

6. MODALITÉS D'ÉTABLISSEMENTS DE RAPPORTS

Les auditeurs rendent compte directement à l'Auditeur général ou à son représentant désigné au sein de son bureau. Des réunions de coordination régulières sont organisées afin de discuter de l'état d'avancement de l'audit, des observations émergentes et des principaux domaines de risque. Les rapports d'audit sont rédigés en anglais dans un langage clair, précis et professionnel, adapté à la direction générale et aux instances de contrôle.

7. QUALIFICATIONS DES CABINETS ET COMPOSITION DE LEUR ÉQUIPE

7.1 Qualifications des consultants :

Chaque cabinet soumissionnaire doit satisfaire aux critères d'éligibilité minimaux énoncés ci-après, en sus des qualifications individuelles du personnel décrites ci-après. Les offres qui n'apportent pas la preuve de leur conformité à ces exigences sont considérées comme non conformes et exclues de toute autre évaluation. Les cabinets de conseil doivent justifier d'une expérience significative en matière d'audit des systèmes d'information, de préférence dans des environnements du secteur public, régionaux ou comptant plusieurs entités et analogues à la CEDEAO. Le cabinet doit :

a) avoir exercé des activités d'audit des systèmes d'information ou de conseil en TIC pendant au moins cinq (5) ans, comme en atteste son acte constitutif ou tout autre document d'enregistrement juridique équivalent ;
b) disposer d'une équipe principale d'audit des systèmes d'information composée d'au moins dix (10) professionnels qualifiés titulaires de certifications reconnues, notamment, mais sans s'y limiter, les certifications CISA, CISSP, CISM ou toute autre certification équivalente reconnue par l'ISACA ou des organismes internationaux comparables ;
c) démontrer qu'il a mené à bien au moins trois (3) missions comparables d'audit des systèmes d'information ou d'assurance des technologies de l'information et de la communication au sein d'institutions du secteur public, d'organisations internationales ou d'environnements comptant plusieurs entités au cours des cinq (5) années précédant la date limite de soumission des offres. Les justificatifs devront être fournis sous forme de lettres de référence, de certificats d'achèvement de mission ou de documents équivalents ;
d) atteindre un seuil minimal de chiffre d'affaires annuel moyen tel que spécifié dans le dossier d'appel d'offres officiel, proportionnel à la valeur estimée du contrat-cadre ;
e) être valablement enregistré ou constitué dans une juridiction satisfaisant aux conditions pour participer aux passations de marchés de la CEDEAO en vertu du Code des marchés de 2021, et ne doit faire l'objet d'aucune mesure d'exclusion, de sanction ou de disqualification en vigueur imposée par une quelconque autorité nationale, régionale ou internationale chargée des marchés publics ;
f) démontrer sa capacité financière à mener à bien la mission ; et
g) être indépendant des institutions de la CEDEAO et de leurs filiales.

7.2 Composition de l'équipe et expertise des ressources :

a) **spécialiste en cybersécurité :** jouir d'une expertise en sécurité des réseaux et des systèmes ; certifications telles que CISSP, CISM ou CEH, CISA ou CRISC, OSCP ou GIAC, auditeur principal ISO 27001, professionnel certifié en sécurité dans le cloud (CCSP), connaissance du cadre NIST.
b) **expert en protection des données et conformité :** disposer d'une bonne connaissance des lois sur la protection des données (par exemple, la NDPA nigériane, le RGPD le cas échéant) ; une certification CIPP/E ou CISSP (module « confidentialité ») constitue un atout ;
c) **auditeur(s) informatique(s) senior(s) :** justifier d'au moins cinq à sept années d'expérience en audit informatique et de solides compétences analytiques. Certification CISA (obligatoire), CIA (atout majeur), CISSP ou CISM, CRISC, certification « Cloud » (dans des environnements modernes) ;

d) **spécialiste senior en sécurité du cloud/architecte :** avoir au moins cinq à sept années d'expérience en audit informatique et de solides compétences analytiques. Détenir une certification CCSP (fortement souhaitée), une certification avancée en sécurité du cloud délivrée par un fournisseur, CISSP ou CISM, auditeur principal ou responsable de la mise en œuvre ISO 27001 ; et

e) **analyste judiciaire :** disposer d'un minimum cinq à sept années d'expérience en audit informatique et de solides compétences analytiques. Avoir une certification GCFA, EnCE ou CFCE, CISSP ou une certification équivalente, une expertise avérée en chaîne de conservation des preuves, ainsi qu'une expérience en matière de procédures disciplinaires ou judiciaires.

Des CV détaillés indiquant les diplômes universitaires, les certifications et l'expérience de missions pertinentes devront être fournis.
Tous les membres clés du personnel proposés doivent être titulaires d'un diplôme universitaire en informatique ou dans des domaines connexes (par exemple, génie logiciel, technologies de l'information (TI), systèmes d'information (SI), génie informatique, cybersécurité, intelligence artificielle (IA), cloud computing), et posséder les certifications professionnelles mentionnées. L'offre doit inclure les CV détaillés des membres clés du personnel, leurs rôles proposés et la confirmation de leur disponibilité. Aucun changement d'experts clés n'est autorisé sans l'accord écrit préalable du Bureau de l'Auditeur Général (BAG).

8. NORMES PROFESSIONNELLES

Le consultant doit se conformer aux normes professionnelles énoncées ci-après, qui définissent les exigences minimales en matière d'éthique, de professionnalisme et de gouvernance applicables à la prestation des services. Ces normes visent à garantir la confidentialité, l'indépendance, l'objectivité, l'intégrité et le respect des normes d'audit internationales applicables ainsi que de la réglementation de la CEDEAO pendant toute la durée de la mission. Elles comprennent :

1) la confidentialité et protection des données : le consultant doit traiter comme strictement confidentielles toutes les informations obtenues dans le cadre de l'exécution du contrat et ne les utilise qu'aux fins de la prestation des services. Il se conforme aux lois applicables en matière de protection des données, aux réglementations de la CEDEAO et aux politiques institutionnelles, et met en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données sensibles et à caractère personnel ;

2) l'indépendance, l'objectivité et la déontologie : le consultant fournit les services en toute indépendance, objectivité, intégrité, compétence professionnelle et diligence, et ce, conformément aux normes reconnues d'audit et d'assurance des systèmes d'information (SI) publiées par l'ISACA ainsi qu'aux autres normes internationales applicables ;

3) la déclaration d'indépendance et d'inexistence de conflit d'intérêts : chaque cabinet soumissionnaire doit présenter, à titre obligatoire dans le cadre de son offre technique et avant la signature du contrat, une déclaration signée d'indépendance et d'inexistence de conflit d'intérêts, confirmant que ni le cabinet ni aucun membre de son équipe chargée de la mission n'entretient de relation financière, de conseil, de consultation ou professionnelle avec une institution, une agence ou un bureau de la CEDEAO susceptible de compromettre son indépendance ou de créer un conflit d'intérêts réel, potentiel ou perçu ;

4) l'obligation continue de divulgation : l'obligation de déclarer les conflits d'intérêts s'applique de manière continue pendant toute la durée du contrat-cadre. Tout conflit réel, potentiel ou perçu qui survient ou dont on prend connaissances doit être signalé sans délai et par écrit au Bureau de l'Auditeur Général (BAG) ;

5) la vérification et les mesures correctives : le BAG se réserve le droit de vérifier toutes les déclarations soumises, de mener les vérifications supplémentaires jugées nécessaires et d'imposer des mesures correctives appropriées, y compris l'exclusion de missions spécifiques, la disqualification ou la résiliation du contrat, en cas d'identification d'un conflit d'intérêts qui n'a pas été convenablement divulgué ou ne peut être atténué à satisfaction ; et

6) les manquements et les sanctions : tout manquement aux présentes normes professionnelles constitue un manquement grave au contrat et peut entraîner la résiliation de celui-ci ou l'application d'autres mesures correctives conformément aux termes du contrat.

9. CONFIDENTIALITÉ ET PROTECTION DES DONNÉES

Le consultant est soumis aux exigences suivantes en matière de confidentialité et de protection des données, qui définissent les obligations relatives à la sauvegarde des informations sensibles, à la protection des données à caractère personnel et au respect des lois applicables, des règlements et des politiques institutionnelles de la CEDEAO pendant toute la durée de la mission :

a) **la confidentialité des informations :** le consultant est tenu de préserver la confidentialité la plus stricte concernant toutes les informations obtenues, consultées ou générées dans le cadre de la prestation des services et n'utilise ces informations qu'aux seules fins de l'exécution du contrat ;
b) **les mesures de protection des données :** le consultant doit se conformer à l'ensemble des lois applicables en matière de protection des données, des règlements et des politiques institutionnelles de la CEDEAO. Il doit mettre en œuvre les mesures techniques et organisationnelles appropriées visant à protéger les données sensibles et à caractère personnel contre tout accès non autorisé, toute divulgation, toute altération ou toute perte ;

c) **l'accord de non-divulgation (AND) obligatoire :** la signature d'un accord de non-divulgation (AND) constitue une condition obligatoire pour l'adjudication du marché. Un projet d'AND sera annexé au dossier d'appel d'offres afin de permettre aux soumissionnaires d'en examiner les dispositions et d'en tenir compte dans leurs offres et leurs estimations de coûts ;
d) **la signature d'un engagement de confidentialité avant l'adjudication du marché :** le BAG se réserve le droit d'exiger des soumissionnaires présélectionnés qu'ils signent un engagement de confidentialité préalable à l'adjudication avant qu'il ne leur soit accordé l'accès à toute information sensible relative à la passation de marché ou à l'institution au cours du processus d'évaluation ou de négociation ;
e) **l'accord de non-divulgation obligatoire en tant qu'annexe au contrat :** lors de l'adjudication du marché, l'accord de non-divulgation signé fait partie intégrante du contrat-cadre et constitue une annexe juridiquement contraignante de celui-ci ;
f) **les signataires de l'accord de non-divulgation :** l'accord de confidentialité doit être signé par le ou les représentant(s) dûment habilité(s) du cabinet de conseil et par chaque membre désigné de l'équipe chargée de la mission avant le début de tout travail sur le terrain ou l'accès à des informations confidentielles. Nul ne peut participer à l'exécution des services tant que son accord de confidentialité signé n'aura pas été remis et accepté par l'autorité contractante ;
g) **les contrats spécifiques et les changements de personnel :** lorsque le contrat-cadre est exécuté par le biais de contrats spécifiques et que du personnel supplémentaire ou de remplacement est affecté à une mission spécifique, chacune de ces personnes doit signer un nouvel accord de confidentialité individuel avant de commencer à travailler dans le cadre de cette commande ponctuelle. Le cabinet de conseil veille au respect intégral de cette exigence ;
h) **le champ d'application et survie des obligations :** les obligations de confidentialité s'appliquent à toutes les informations obtenues, consultées ou générées dans le cadre de la prestation des Services et subsistent pendant une période de trois (3) ans à compter de l'expiration ou de la résiliation du contrat, sauf si l'accord de non-divulgation prévoit une durée plus longue ou si la législation en vigueur l'exige ; et
i) **les manquements et les recours :** tout manquement aux obligations de confidentialité ou aux obligations découlant de l'accord de non-divulgation de la part du cabinet de conseil ou de son personnel constitue un manquement grave au contrat et peut entraîner la suspension immédiate des services et, le cas échéant, la résiliation du contrat, sans préjudice de tout autre recours contractuel, légal ou recours équitables dont dispose le pouvoir adjudicateur.

10. TRANSFERT DE CONNAISSANCES ET RENFORCEMENT DES CAPACITÉS

Afin de promouvoir la durabilité et le renforcement institutionnel, le consultant :

a) organise des ateliers structurés de partage des connaissances à l'intention du personnel du BAG ;

b) partage les méthodologies, les outils et les modèles utilisés lors des audits ;
c) fournit des analyses et des enseignements tirés de l'expérience afin de renforcer les capacités internes d'audit des systèmes d'information ; et
d) encourage la participation collaborative du personnel du BAG lors des activités sur le terrain.

Le transfert de connaissances est intégré à l'approche globale de l'audit afin d'en garantir la valeur durable.

11. INDICATEURS CLÉS DE PERFORMANCE (ICP)

#	ICP	OBJECTIF
1	Remise des livrables dans les délais	≥ 95 % dans les délais convenus
2	Note de qualité attribuée par le BAG	Note de satisfaction ≥ 85 %
3	Taux d'acceptation des recommandations	≥ 90 %
4	Taux de mise en œuvre des recommandations	≥ 75 % dans les délais impartis
5	Séances de transfert de connaissances	Au moins 2 par an

12. MATRICE D'ÉVALUATION TECHNIQUE

#	CRITÈRES	COEFFICIENT (%)	BASE
1	Expérience du cabinet	10	Pertinence et complexité des missions
2	Méthodologie et approche	30	Robustesse et conformité aux normes
3	Principaux experts	40	Certifications et expérience
4	Plan de transfert des connaissances	10	Stratégie de renforcement des capacités
5	Participation du personnel des pays membres de la CEDEAO	10	Participation du personnel des États membres de la CEDEAO
	TOTAL	**100**	

Note minimale requise pour la qualification technique : 75 %. Les offres financières ne seront ouvertes que pour les cabinets techniquement qualifiés.

Évaluation financière et notation combinée

L'évaluation des offres se fait selon la méthode de sélection fondée sur la qualité et le coût (QCBS). La qualité technique a un coefficient de pondération de quatre-vingts pour cent (80 %) et l'offre financière un coefficient de vingt pour cent (20 %). Seuls les cabinets ayant obtenu ou dépassé la note minimale de qualification technique de 75 % verront leurs offres financières ouvertes et évaluées. La note combinée de chaque cabinet éligible est déterminée comme suit :

note combinée = (note technique × 80 %) + (note financière × 20 %)

La note financière de chaque cabinet est calculée en exprimant l'offre financière la plus basse évaluée sous forme de pourcentage par rapport à l'offre de ce cabinet (c'est-à-dire : prix le plus bas évalué ÷ prix proposé par le cabinet × 100). Les deux cabinets ayant obtenu les notes combinées les plus élevées sont recommandés pour l'adjudication du contrat-cadre. En cas d'égalité des notes combinées entre deux cabinets, celui présentant la meilleure note technique est classé en première position.

13. DURÉE DE LA MISSION

Le contrat-cadre s'étend sur une période de trois ans à compter de la date de signature du contrat. La mission fonctionne selon un système de contrats spécifiques, le BAG émettant des commandes spécifiques au fur et à mesure que le soutien en matière d'audit des systèmes d'information sera nécessaire. Chaque contrat spécifique précise la nature du soutien requis, le personnel à déployer, la durée estimée et le lieu d'intervention.

Aucun volume minimum de contrats spécifiques n'est garanti dans le cadre de cet accord-cadre. Le BAG se réserve le droit de déployer le personnel du cabinet pour qu'il travaille sous sa supervision ou, sur instruction spécifique, pour qu'il mène des missions d'audit des systèmes d'information en toute indépendance.

14. CALENDRIER DE PAIEMENT

Les paiements sont effectués sur la base du temps et des efforts consacrés, conformément aux taux journaliers convenus et indiqués dans l'offre financière. Les factures sont soumises mensuellement par le cabinet, accompagnées de feuilles de temps certifiées détaillant le personnel déployé, les jours ouvrés et les tâches effectuées. Le paiement sera traité dans un délai de trente (30) jours calendaires à compter de la certification par le BAG de la feuille de temps concernée. La structure de paiement suivante s'applique :

a) **paiement mensuel sur la base des feuilles de temps :** payable mensuellement après certification par le BAG des feuilles de temps soumises par le cabinet, détaillant le personnel mobilisé, les jours-homme travaillés et les tâches effectuées dans le cadre de chaque ordre de mobilisation en cours ;
b) **missions d'audit indépendantes :** lorsque le BAG demande expressément au cabinet de mener une mission d'audit indépendant des systèmes d'information, un accord de contrat spécifique et distinct est établi, définissant le périmètre, le calendrier, le coût convenu par jour-homme ou le montant forfaitaire, ainsi que les échéances de paiement correspondantes applicables à cette mission spécifique ;
c) **pas d'acomptes :** aucun frais de mobilisation, ni aucun acompte n'est versé au titre du contrat-cadre. Les obligations de paiement ne naissent qu'à compter de l'émission d'un bon de commande pour contrat spécifique et de la prestation certifiée des services qui en découlent ;
d) **feuilles de temps contestées :** lorsque le BAG conteste un élément d'une feuille de temps soumise, la partie non contestée est certifiée et traitée en vue de son règlement dans le délai standard de trente (30) jours calendaires, tandis que la partie contestée est réglée par le biais du mécanisme de règlement des litiges prévu dans le contrat ; et
e) **frais et remboursements :** les frais remboursables, le cas échéant, ne sont payables que s'ils ont été expressément approuvés au préalable par écrit par le Bureau de l'Auditeur Général (BAG) et justifiés par des reçus originaux. Les frais de déplacement, d'hébergement et de subsistance sont régis par les tarifs applicables aux consultants de la CEDEAO ou selon les modalités convenues dans l'accord-cadre ou dans le bon de commande du contrat spécifique correspondant.