Ref: ECW/OAG/ADM/06-26-103/oja Date: 17th June 2026

REQUEST FOR PROPOSALS

PROVISION OF INFORMATION SYSTEMS (IS) AUDIT SERVICES

The Office of the Auditor General of ECOWAS Institutions (OAG) hereby invites qualified and experienced audit firms to submit Technical and Financial Proposals for the provision of Information Systems (IS) Audit Services under a three-year Framework Agreement.

The assignment seeks to support the Office of the Auditor General in conducting risk-based Information Systems audits across ECOWAS Institutions, Agencies, and Offices. The services will cover areas including ICT governance, cybersecurity, risk management, information security, data governance, business continuity and disaster recovery, enterprise applications, regulatory compliance, and other related information systems audit activities.

IMPORTANT NOTICE

Interested firms are strongly advised to carefully review the attached Terms of Reference (TOR) before preparing and submitting their proposals. The TOR forms an integral part of this solicitation and contains detailed information regarding the scope of services, eligibility requirements, consultant qualifications, technical evaluation criteria, methodology, deliverables, reporting arrangements, payment terms, and contractual obligations.

Submission of a proposal shall be deemed as confirmation that the bidder has reviewed, understood, and accepted the requirements and conditions set out in the TOR.

ELIGIBILITY

Eligible firms must demonstrate substantial experience in Information Systems Auditing and possess the requisite technical expertise, professional certifications, and

resources required to undertake assignments of this nature, as detailed in the attached TOR.

SUBMISSION REQUIREMENTS

Interested firms shall submit the following:

- Technical Proposal
- Financial Proposal
- Company Profile
- Evidence of Relevant Experience
- Supporting Eligibility Documents and Certifications as specified in the TOR.

SUBMISSION METHOD AND DEADLINE

Proposals may be submitted electronically or delivered in hard copy to the address indicated below:

Electronic Submission: oag-procurement-lcb@ecowas.int

Physical Submission: Office of the Auditor General of ECOWAS Institutions, 10 Dar es Salam Crescent Wuse 2, Abuja, Nigeria.

Deadline: All proposals must be received no later than 25th July 2026.

IMPORTANT INSTRUCTIONS

- Electronic submissions shall bear the subject line: **"Proposal for Provision of Information Systems (IS) Audit Services – Ref: ECW/OAG/ADM/06-26-103/oja**
- Bidders must ensure that their proposals fully address all requirements contained in the attached TOR.
- Failure to provide the information, qualifications, supporting documentation, or certifications required under the TOR may result in the proposal being declared non-responsive.
- Late submissions shall not be considered.
- The Office of the Auditor General reserves the right to accept or reject any proposal and is not bound to award a contract as a result of this solicitation.
- The issuance of this Request for Proposals does not constitute a commitment by the OAG to award a contract or to reimburse any costs incurred in the preparation and submission of proposals.

REQUESTS FOR CLARIFICATION

Any request for clarification regarding this procurement process shall be submitted in writing to:
oag-is-procurement@ecowas.int

THE OFFICE OF AUDITOR GENERAL OF ECOWAS INSTITUTIONS (OAG)

TERMS OF REFERENCE (TOR)

PROVISION OF INFORMATION SYSTEMS (IS) AUDIT SERVICES

CONTENTS

1. BACKGROUND AND CONTEXT

At the heart of the ECOWAS Vision 2050 is a community of people integrated in a peaceful, prosperous region, with strong institutions that respect fundamental freedoms and work for inclusive and sustainable development. In this connection, the President of the ECOWAS Commission is to mobilize the citizens of the region to the vision and help to achieve it by 2050.

The Office of the Auditor General (OAG) was created in 2018 by the Authority of Heads of State and Government, following an Institutional Reform exercise, as an Independent Oversight Institution. As part of the commitment to improve the West Africa integration process while enhancing its effectiveness, the Office of the Auditor General is to ensure transparency and accountability of all ECOWAS Institutions, Agencies and Offices.

Following the approval of a strategic plan, the Office of the Auditor General intends to engage an audit firm in a three-year framework contract to support the Office in the audits of ECOWAS Institutions, Agencies, and Offices, which included IT/system reviews among other assignments. The OAG intents to apply part of its annual budget allocations to engage an independent firm in a framework agreement to provide Information Systems (IS) Audit services under an open regional competitive bidding process for the next three-year period (commencing June 2026).

The objective of this engagement is to ensure that ECOWAS's ICT environment remains secure, resilient, well-governed, and fully aligned with internationally recognized standards, frameworks, and regulatory requirements applicable to ECOWAS. Therefore, under the oversight of the OAG, the appointed Information Systems Audit Firm shall collaborate with the OAG, with office in Abuja, Nigeria, to assess and strengthen all ECOWAS Institutions, Agencies, and Office's IT governance, cybersecurity posture, internal control systems, and enterprise risk management processes.

This assignment, together with the resulting contractual obligations, shall be governed by the Procurement Code, 2021 and the ECOWAS Financial Regulations, 2021. Accordingly, all procurement, implementation, and reporting processes shall adhere strictly to established principles of public procurement, including open competitive bidding, transparency, accountability, and non-discrimination.

2. OBJECTIVES OF THE ASSIGNMENT

The objectives of the IS Audit engagement are to provide independent, objective, and evidence-based assurance regarding the adequacy, effectiveness, and maturity of ICT governance, risk management, cybersecurity, and control environments.

Specifically, the assignment aims to:

Evaluate whether existing ICT governance frameworks—including structures, policies, processes, and oversight mechanisms—are functioning effectively and supporting the institutional mandate.

Identify systemic vulnerabilities, control deficiencies, cybersecurity exposures, compliance gaps, and process inefficiencies that may impact organizational performance or resilience.

Benchmark current ICT practices, processes, and controls against established international standards and frameworks such as COBIT 2019, ISO/IEC 27001 and 27002, the NIST Cybersecurity Framework, ITIL 4, and applicable ISSAI guidance.

Provide actionable, prioritized, and risk-based recommendations to strengthen ICT resilience, enhance control maturity, and improve operational efficiency and reliability.

Support oversight bodies and senior management in reinforcing accountability, transparency, and long-term performance sustainability within the ICT environment.

Promote and safeguard the confidentiality, integrity, availability, and overall reliability of ECOWAS information assets, digital platforms, and enterprise systems.

3. SCOPE OF SERVICES

The selected Information Systems Audit Firms shall undertake annual, risk-based IS Audit assignments that encompass, but are not limited to, the following domains:

a. IT Governance and Strategic Alignment:

Assess the adequacy and effectiveness of ICT governance frameworks, decision-making structures, steering mechanisms, policy instruments, accountability arrangements, and the alignment of ICT strategies, architectures, and investments with the institutional mission and operational objectives.

b. ICT Risk Management:

Evaluate risk identification methodologies, assessment processes, prioritization criteria, mitigation and monitoring practices, and the completeness and quality of ICT risk registers. Confirm that risk treatment measures are appropriate and proportionate to exposure levels.

c. Information Security Management:

Assess the design and operational effectiveness of policies, procedures, and controls that safeguard the confidentiality, integrity, and availability of information assets. This includes identity and access management, configuration hardening, system logging and monitoring, security baselines, and vulnerability remediation processes.

d. Cybersecurity Posture Assessment:
Evaluate the adequacy of network, platform, and endpoint security controls, including perimeter defences, firewall and IDS/IPS configurations, endpoint detection and response capabilities, patch and update management, physical safeguards, and incident detection, response, and escalation processes, in alignment with NIST Cybersecurity Framework principles.

e. IT Service Management (ITSM):
Review IT operational processes such as incident and problem management, change and release management, configuration and asset management, service desk operations, service continuity arrangements, and service level performance monitoring, in accordance with ITIL 4 best practices.

f. Data Governance, Protection, and Privacy:
Assess data lifecycle controls—including creation, classification, storage, transmission, archival, retention, and disposal—along with data quality, stewardship structures, governance accountability, and compliance with applicable regional and international data protection requirements.

g. Business Continuity and Disaster Recovery (BCP/DR):
Examine continuity plans, disaster recovery architectures, backup strategies, RTO/RPO definitions, off-site storage arrangements, and evidence of periodic testing, restoration drills, and readiness assessments.

h. IT Projects, Digital Initiatives, and Change Management:
Evaluate governance arrangements for system development, procurement, implementation, migration, configuration changes, and post-implementation reviews. Confirm the existence of appropriate segregation of duties, environment controls, and stakeholder engagement mechanisms.

i. Enterprise Applications and Platforms:
Audit general IT controls (GITCs) and application-level controls for critical enterprise systems—including SAP ERP, financial management systems, HR platforms, and specialized applications—covering access rights, configurable controls, audit logging, data integrity, and change control mechanisms.

j. ICT Compliance Reviews:
Assess compliance with internal ICT policies, procedures, regulatory obligations, licensing arrangements, and external requirements applicable to ICT operations, including donor guidelines and regional mandates.

k. AI Governance and Strategic Alignment:

Conduct risk-based AI audit engagements to evaluate the design and effectiveness of AI governance frameworks, oversight and ethical review structures, decision-rights allocation, accountability mechanisms, and policies governing AI development, procurement, deployment, monitoring, and lifecycle management. Assess the alignment of AI strategy, investment planning, data use, and innovation initiatives with institutional objectives, regulatory expectations, ethical standards, and enterprise risk management principles to support responsible and value-driven AI adoption.

l. Regulatory and Policy Compliance:

Verify adherence to applicable legal, regulatory, and policy requirements—including regional financial rules, donor compliance conditions, intellectual property laws, technology licensing terms, and open-source usage obligations—as they relate to ICT operations and service delivery.

m. Specialized and Ad-hoc Reviews:

Perform targeted reviews, post-incident analyses, and emerging technology audits based on specific requests from the Office of the Auditor General (OAG).

n. Other Focus Areas:

Undertake specialized, thematic, or ad-hoc reviews as requested, such as audits of cybersecurity incidents, new technology deployments, emerging risk areas, or follow-up assessments of prior audit recommendations.
The scope of services shall apply to all ECOWAS Institutions, Agencies, and Field Offices covered under the ECOWAS institutional framework.

4. METHODOLOGY AND APPROACH

The auditor shall apply a structured, risk-based, and evidence-driven audit methodology aligned with ISACA IS Audit & Assurance Standards and other internationally recognized assessment frameworks. The approach shall encompass inception planning, comprehensive risk, development of detailed audit programs, fieldwork and technical testing, risk rating of findings (e.g., Critical/High/Moderate/Low), preparation of draft and final reports, and systematic follow-up reviews to assess implementation of recommendations.

The methodology shall include:

a. Comprehensive planning and risk assessment in consultation with key stakeholders.
b. Development of detailed audit programs and control criteria.
c. Fieldwork involving interviews, walkthroughs, documentation review, sampling, analytics, and technical testing where appropriate.
d. Maintenance of traceable, verifiable audit working papers supporting conclusions.
e. Risk rating of observations based on impact and likelihood considerations.

f. Validation discussions with management to confirm factual accuracy.
g. Preparation of structured draft and final audit reports.
h. Follow-up activities to assess implementation status of agreed remediation actions.

The approach shall emphasize professional scepticism, independence, objectivity, and quality assurance throughout the audit cycle.

5. DELIVERABLES

The auditor shall produce the following technical outputs:

a. Annual Risk-Based IS Audit Plan outlining engagements, scope focus areas, and indicative timelines.
b. Engagement-Level Audit Work Programs describing objectives, criteria, and procedures.
c. Periodic Progress Reports summarizing status, key issues, and emerging risks.
d. Draft IS Audit Reports including executive summary, background, scope, methodology, detailed findings, risk ratings, and recommendations.
e. Final IS Audit Reports incorporating management responses and agreed action plans.
f. Presentation and briefing sessions for the OAG and relevant stakeholders.
g. Complete electronic working papers and supporting documentation sufficient for OAG review and retention.

All deliverables shall be clear, structured, evidence-based, and aligned with professional reporting standards.

6. REPORTING ARRANGEMENTS

The shall report directly to the Auditor General or designated representative within auditor the OAG. Regular coordination meetings shall be conducted to discuss audit progress, emerging observations, and key risk areas.
Audit reports shall be prepared in English using clear, precise, and professional language suitable for executive management and oversight bodies.

7. CONSULTANT QUALIFICATIONS AND TEAM COMPOSITION

7.1 Consultant Qualification:

Each bidding firm shall satisfy the following minimum eligibility requirements, in addition to the individual staff qualifications that follows. Proposals that fail to demonstrate compliance with these requirements shall be deemed non-responsive and excluded from further evaluation. Consulting firms must demonstrate substantial experience in Information Systems auditing, preferably within public-sector, regional, or multi-entity environments comparable to ECOWAS:

a. The firm shall have been engaged in Information Systems audit or ICT advisory services for a minimum of five (5) years, evidenced by its certificate of incorporation or equivalent legal registration documentation.
b. The firm shall maintain a core IS audit team of not fewer than ten (10) qualified professionals holding recognized certifications, including but not limited to CISA, CISSP, CISM, or equivalent designations recognized by ISACA or comparable international bodies.
c. The firm shall demonstrate successful completion of a minimum of three (3) comparable IS audit or ICT assurance engagements within public sector institutions, international organizations, or multi-entity environments within the five (5) years preceding the submission deadline. Evidence shall be provided in the form of reference letters, engagement completion certificates, or equivalent documentation.
d. The firm shall meet a minimum average annual turnover threshold as specified in the formal tender documentation, proportionate to the estimated value of the framework contract.
e. The firm shall be validly registered or incorporated in a jurisdiction eligible to participate in ECOWAS procurement under the Procurement Code, 2021, and shall not be subject to any current debarment, sanction, or disqualification imposed by any national, regional, or international procurement authority.
f. Demonstrate financial capacity to execute the assignment.
g. Be independent from ECOWAS institutions and their subsidiaries.

7.2 Team composition and Resource Expertise.

a. **Cybersecurity Specialist**: Expertise in network/system security; certifications like CISSP, CISM or CEH, CISA or CRISC, OSCP or GIAC, ISO 27001 Lead Auditor, Certified Cloud Security Professional (CCSP), NIST framework familiarity.
b. **Data Privacy/Compliance Expert**: Knowledgeable about data protection laws (e.g., Nigeria NDPA, GDPR if applicable); certification CIPP/E or CISSP (privacy module) is a plus.
c. **Senior IT Auditor(s):** At least 5–7 years of IT auditing experience, and strong analytical skills. CISA (mandatory), CIA (strong advantage), CISSP or CISM, CRISC, Cloud certification (in modern environments)
d. **Senior Cloud Security Specialist / Architect**: At least 5–7 years of IT auditing experience, and strong analytical skills. CCSP (strongly expected), One advanced vendor cloud security certification, CISSP or CISM, ISO 27001 Lead Auditor/Implementer.
e. **Forensic Analyst**: At least 5–7 years of IT auditing experience, and strong analytical skills. GCFA or equivalent, EnCE or CFCE, CISSP, demonstrated chain-of-custody expertise, Experience supporting disciplinary or legal proceedings.

Detailed CVs outlining academic qualifications, certifications, and relevant engagement experience shall be provided.

All proposed key staff must have university degrees in Computer Science or related fields (e.g., Software Engineering, Information Technology (IT), Information Systems (IS), Computer Engineering, Cybersecurity, Artificial Intelligence (AI), Cloud Computing), with professional certifications as noted. The bid must include detailed CVs of key personnel, their proposed roles, and confirmation of their availability. No changes to key experts will be allowed without the OAG's prior written consent.

8. PROFESSIONAL STANDARDS

The Consultant shall adhere to the following Professional Standards, which define the minimum ethical, professional, and governance requirements applicable to the performance of the Services. These standards are intended to ensure confidentiality, independence, objectivity, integrity, and compliance with applicable international audit standards and ECOWAS regulations throughout the duration of the engagement. These include:

1. Confidentiality and Data Protection: The Consultant shall treat as strictly confidential all information obtained in the performance of the Contract and shall use such information solely for the purposes of executing the Services. The Consultant shall comply with applicable data protection laws, ECOWAS regulations, and institutional policies, and shall implement appropriate technical and organizational measures to safeguard sensitive and personal data.

2. Independence, Objectivity, and Professional Conduct: The Consultant shall perform the Services with full independence, objectivity, integrity, professional competence, and due care, and in accordance with recognized IS Audit and Assurance Standards issued by ISACA and other applicable international standards.

3. Declaration of Independence and Conflict of Interest: Each bidding firm shall submit, as a mandatory component of its technical proposal and prior to contract signature, a signed Declaration of Independence and Absence of Conflict of Interest, confirming that neither the firm nor any member of its engagement team has any financial, advisory, consultancy, or professional relationship with any ECOWAS Institution, Agency, or Office that could impair independence or create a real, potential, or perceived conflict of interest.

4. Ongoing Disclosure Obligation: The obligation to disclose conflicts of interest shall be continuous throughout the duration of the framework contract. Any actual, potential, or perceived conflict that arises or becomes known shall be promptly disclosed in writing to the Office of the Auditor-General (OAG).

5. Verification and Remedial Actions: The OAG reserves the right to verify all declarations submitted, conduct additional due diligence as deemed necessary, and impose appropriate remedial measures, including exclusion from specific engagements, disqualification, or termination of the contract, where a conflict of interest is identified, inadequately disclosed, or cannot be satisfactorily mitigated.

6. Breach and Sanctions: Any breach of these Professional Standards shall constitute a material breach of contract and may result in termination or the application of other remedies in accordance with the terms of the Contract.

9. CONFIDENTIALITY AND DATA PROTECTION

The Consultant shall be subject to the following Confidentiality and Data Protection requirements, which establish the obligations for safeguarding sensitive information, protecting personal data, and ensuring compliance with applicable laws, ECOWAS regulations, and institutional policies throughout the duration of the engagement:

a. **Confidentiality of Information**: The Consultant shall maintain strict confidentiality over all information obtained, accessed, or generated in the performance of the Services and shall use such information solely for the purposes of executing the Contract.
b. **Data Protection Safeguards**: The Consultant shall comply with all applicable data protection laws, ECOWAS regulations, and institutional policies, and shall implement appropriate technical and organizational measures to protect sensitive and personal data against unauthorized access, disclosure, alteration, or loss.
c. **Mandatory Non-Disclosure Agreement (NDA):** Execution of a Non-Disclosure Agreement (NDA) shall be a mandatory condition of contract award. A draft NDA shall be annexed to the tender documentation to enable bidders to review and factor its requirements into their proposals and cost estimates.
d. **Pre-Award Confidentiality Undertaking:** The OAG reserves the right to require shortlisted bidders to execute a pre-award confidentiality undertaking prior to granting access to any sensitive procurement or institutional information during the evaluation or negotiation process.
e. **NDA as Contract Annex:** At contract award, the executed NDA shall form an integral and legally binding annex to the framework contract.
f. **NDA Signatories:** The NDA shall be signed by the duly authorized representative(s) of the consulting firm and by each named member of the engagement team prior to the commencement of any fieldwork or access to confidential information. No individual shall participate in the performance of the Services until their signed NDA has been submitted and accepted by the Contracting Authority.
g. **Call-Offs and Personnel Changes:** Where the framework contract is implemented through call-off arrangements and additional or replacement personnel are assigned to a specific engagement, each such individual shall execute a new individual NDA prior to commencing work under that call-off. The consulting firm shall ensure full compliance with this requirement.
h. **Scope and Survival of Obligations:** Confidentiality obligations shall apply to all information obtained, accessed, or generated in connection with the performance of the Services and shall survive the expiration or termination of the Contract for

a period of three (3) years thereafter, unless a longer period is specified in the NDA or required by applicable law.

i. **Breach and Remedies:** Any breach of confidentiality or NDA obligations by the consulting firm or its personnel shall constitute a material breach of contract and may result in immediate suspension of the Services and, where appropriate, termination of the Contract, without prejudice to any other contractual, legal, or equitable remedies available to the Contracting Authority.

10. KNOWLEDGE TRANSFER AND CAPACITY DEVELOPMENT

To promote sustainability and institutional strengthening, the consultant shall:

a. Conduct structured knowledge-sharing workshops for OAG staff.
b. Share methodologies, tools, and templates applied during audits.
c. Provide insights and lessons learned to enhance internal IS audit capability.
d. Encourage collaborative participation of OAG staff during fieldwork activities.

Knowledge transfer shall be integrated into the overall audit approach to ensure lasting value.

11. KEY PERFORMANCE INDICATORS (KPIS)

#	KPI	TARGET
1	Timely submission of deliverables	≥ 95% within agreed timelines
2	Quality rating by OAG	≥ 85% satisfaction score
3	Recommendation acceptance rate	≥ 90%
4	Implementation rate of recommendations	≥ 75% within timeframe
5	Knowledge transfer sessions	Minimum 2 per year

12. TECHNICAL EVALUATION MATRIX

#	CRITERIA	WEIGHT (%)	BASIS

1	Firm Experience	10	Relevance and complexity of assignments
2	Methodology and Approach	30	Robustness and standards alignment
3	Key Experts	40	Certifications and experience
4	Knowledge Transfer Plan	10	Capacity building strategy
5	ECOWAS Member Country Personnel Participation	10	Participation of ECOWAS Member State personnel
	TOTAL	**100**	

Minimum technical qualifying score: 75%. Financial proposals will be opened only for technically qualified firms.

Financial Evaluation and Combined Scoring

The evaluation of proposals shall be conducted on a Quality- and Cost-Based Selection (QCBS) basis. Technical quality shall carry a weight of eighty percent (80%) and the financial proposal a weight of twenty percent (20%). Only firms that attain or exceed the minimum technical qualifying score of 75% shall have their financial proposals opened and evaluated. The combined score for each qualifying firm shall be determined as follows:

Combined Score = (Technical Score × 80%) + (Financial Score × 20%)

The financial score of each firm shall be derived by expressing the lowest evaluated financial proposal as a percentage of that firm's own proposal (i.e., Lowest Evaluated Price ÷ Firm's Price × 100). The two firms attaining the highest combined scores shall be recommended for award of the framework contract. Where two firms achieve equal combined scores, the firm with the superior technical score shall be ranked first.

13. DURATION OF ASSIGNMENT

The framework agreement shall span a three-year period commencing from the date of contract signature. The engagement shall operate on a call-off basis, with the OAG issuing specific call-off orders as and when IS audit support is required. Each call-off shall specify the nature of support required, the personnel to be deployed, the estimated duration, and the applicable location.

No minimum volume of call-offs is guaranteed under this framework. The OAG reserves the right to deploy the firm's staff to work under OAG supervision or, where specifically directed, to conduct independent IS audit assignments.

14. PAYMENT SCHEDULE

Payments shall be made on a time-and-effort basis in accordance with the agreed man-day rates established in the financial proposal. Invoices shall be submitted monthly by the firm, supported by certified timesheets detailing personnel deployed, days worked, and tasks performed. Payment shall be processed within thirty (30) calendar days of OAG certification of the relevant timesheet. The following payment structure shall apply:

a. **Monthly Timesheet Payment:** Payable monthly upon OAG certification of timesheets submitted by the firm, detailing personnel deployed, man-days worked, and tasks performed under each active call-off order.
b. **Independent Audit Assignments:** Where the OAG specifically requests the firm to conduct an independent IS audit engagement, a separate call-off agreement shall be issued defining the scope, timeline, agreed man-day cost or lump-sum, and corresponding payment milestones applicable to that specific engagement.
c. **No Advance Payments:** No mobilization fee or advance payment shall be made under the framework agreement. Payment obligations arise only upon the issuance of a call-off order and the certified delivery of services thereunder.
d. **Disputed Timesheets:** Where the OAG disputes any element of a submitted timesheet, the undisputed portion shall be certified and processed for payment within the standard thirty (30) calendar day period, while the disputed portion is resolved through the contract's dispute resolution mechanism.
e. **Expenses and Reimbursements:** Reimbursable expenses, if any, shall only be payable where expressly pre-approved in writing by the OAG and supported by original receipts. Travel, accommodation, and subsistence costs shall be governed by applicable ECOWAS consultant rates or as otherwise agreed in the framework agreement or the relevant call-off order.