



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

REQUEST FOR EXPRESSIONS OF INTEREST (CONSULTING SERVICES – INDIVIDUAL CONSULTANTS)

COUNTRY: NIGERIA

NAME OF PROJECT: WESTERN AFRICA REGIONAL DIGITAL INTEGRATION PROGRAM (WARDIP)

Grant No.: E264-3W

Assignment Title: Revision of the Directive C/DIR 1/08/11 on fighting cybercrime within ECOWAS.

Reference No. NG-WARDIP-ECOWAS-471324-CS-INDV

The Commission of the Economic Community of West African States (ECOWAS Commission) has received financing from the World Bank toward the implementation of the **Western Africa Regional Digital Integration Program (WARDIP)** and intends to apply part of the proceeds for consulting services.

The consulting services (“the Services”) include review and update of the Directive C/DIR 1/08/11 on the Fight Against Cybercrime to enhance its relevance and effectiveness in combating emergent cybercrimes. This revision aims to align the Directive with recent international norms and standards. The assignment is expected to be completed within twenty (20) weeks.

The detailed Terms of Reference (TOR) for the assignment can be found at the following website:
https://www.ecowas.int/procurement/procurement_m/intellectual-services/

The ECOWAS Commission now invites eligible Individual Consultants (“Consultants”) to indicate their interest in providing the Services. Interested Consultants should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services. The qualifications and relevant experience of the consultants must be supported by documents such as **signed Curricula Vitae (with references), degrees, training certificates, contracts, certificates of performance, etc.** The **ECOWAS Commission reserves the right to reject any application that is not accompanied by the required supporting documents.**

The evaluation criteria are:

Qualifications and skills (support with evidence):

- Possess at least a bachelor’s or master’s degree in law, ICT Law, International Law, or a related legal field relevant to the assignment.
- Additional qualifications or training relevant to the assignment will be highly appreciated.
- Exhibit excellent skills in oral communication, report writing, presentations, and workshop facilitation.

Professional experience (support with evidence):

- Possess at least seven (7) years of professional experience or equivalent demonstrable expertise in the field of cybercrime as relevant to this assignment.

JP.

- Demonstrate a proven track record in developing and revising legal and regulatory frameworks for international or regional organizations. This should include examples of successful projects, publications, or contributions to significant legal reforms.
- Exhibit knowledge of the legal instruments of sub-regional, continental and international organizations to which ECOWAS Member States are parties, in the field of cybersecurity, cybercrime, protection of personal data, privacy laws and cross border data sharing frameworks.

Language:

- The Consultant must demonstrate proficiency in at least more than one official languages of ECOWAS (English, French and Portuguese). Proficiency in a third language is an added advantage.

The attention of interested Consultants is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" September 2023 ("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.

A Consultant will be selected in accordance with the **Individual Consultant selection method** set out in the World Bank Procurement Regulations.

Further information can be obtained at the email addresses below during office hours **0900 to 1700 hours, Nigerian Time (GMT + 1)**.

Expressions of interest must be delivered in a written form to the addresses below by e-mail by **February 17, 2025, at 5:00 p.m. Nigerian Time (GMT + 1)**.

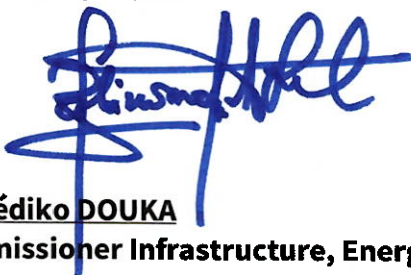
ECOWAS Commission

Attention: Commissioner Infrastructure, Energy and Digitalization

Abuja, Nigeria

E-mail: wardiprecruitment@ecowas.int and copy pbessi@ecowas.int; bahibra@yahoo.fr; mamoa@ecowas.int; folagunju@ecowas.int; msene@ecowas.int; ikkamara@ecowas.int; sbangoura@ecowas.int.

Date: **January 30, 2025**



Mr. Sédiko DOUKA

Commissioner Infrastructure, Energy and Digitalization

Attachment: ToR of the assignment



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Terms of Reference: Revision of the Directive C/DIR 1/08/11 on fighting cybercrime within ECOWAS

1. Background

Digital technologies are transforming lives in the region, increasing connectivity and opportunities but also presenting security challenges. Cybercrime incidents have surged, with Africa experiencing the highest average weekly cyber-attacks per organization in the second quarter of 2023, a 23% increase from 2022¹.

Interpol identified the top cyber threats in Africa as online scams, digital extortion, business email compromise (BEC), ransomware, and phishing². Africa is home to 60% of the world's BEC perpetrators, with six of the most impacted countries situated in West Africa³. The Interpol African cyberthreat Assessment report 2024 confirms these threats remain prevalent⁴.

Countries have enacted cybercrime laws, but the evolving nature of cyber threats requires continuous updates. The 2011 ECOWAS Directive on fighting cybercrime aimed to harmonise laws across West Africa but needs revision to address new challenges and human rights concerns.

The original directive lacked safeguards for law enforcement practices and international cooperation, raising human rights issues. Balancing security measures with individual rights is crucial, requiring updated law enforcement powers at national and regional levels.

ECOWAS emphasises regional integration and cooperation among Member States. Harmonised legal frameworks are essential for combating digital and cybercrimes such as ransomware or cryptocurrency-based crimes, facilitating collaboration in law enforcement, intelligence sharing, and judicial processes.

Several ECOWAS member states have engaged in international treaties on cybercrime. Analysing these instruments and incorporating best practices is necessary.

¹ <https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/>

² <https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa>

³ Agari, The Geography of BEC. The Global Reach of the World's Top Cyber Threat, 2020. Available at: [\[https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf\]](https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf)

⁴ https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf



Revising the Directive ensures its relevance and effectiveness in mitigating and combating emerging cybercrimes. The ECOWAS Commission seeks an individual consultant to review and update Directive C/DIR 1/08/11 on the Fight Against Cybercrime.

2. Objectives and Scope of Work

2.1. General Objective

The objective is to review and amend Directive C/DIR 1/08/11 on the Fight Against Cybercrime to enhance its relevance and effectiveness in combating emergent cybercrimes. This revision aims to align the Directive with recent international norms and standards.

2.2. Scope of Work

The revision process will involve:

- a. Conduct a thorough evaluation of the existing 2011 Directive to identify gaps, inconsistencies, and areas for improvement.
- b. Assess the effectiveness and adequacy of the current provisions within Directive C/DIR 1/08/11.
- c. Align the Directive with international and regional frameworks, standards and practices such as the United Nations Convention Against Cybercrime, African Union Convention on Cybersecurity and Data Protection (The Malabo convention), The Budapest Convention on Cybercrime and its First and Second Additional Protocols.
- d. Studying cybercrime frameworks in Africa and globally to capture best practices, principles and concepts for revising and modernising the Directive.
- e. Ensure that the Directive accommodates technological advancements and allows for increased use of technology in relation to cybercrimes.
- f. Draft the updated provisions to address identified gaps and emerging threats.
- g. Facilitate consultations and workshops to gather input and feedback.
- h. Finalise the revised directive for adoption by ECOWAS member states.

The consultant is expected to consult with all relevant national and regional stakeholders.

3. Deliverables and timeline

3.1. Deliverables and timeline for implementation of services

The assignment is expected to be completed within **twenty (20) weeks**, following the indicative timetable below:

#	Deliverables	Timeline
1	Submission of Inception report	Signing of contract + 2 Weeks
2	Validation of inception report by ECOWAS Commission	Signing of contract + 4 Weeks



#	Deliverables	Timeline
3	Submission of findings from analysis of existing directive, benchmarking report and initial draft of the revised directive	Signing of contract + 8 Weeks
4	Validation of initial draft of revised directive (workshop & report)	Signing of contract + 11 Weeks
5	Submission of final directive	Signing of contract + 15 Weeks
6	Validation of finalised draft of revised directive (workshop & report)	Signing of contract + 18 Weeks
7	Submission of final directive (incorporate feedback)	Week 20

3.2. Format of Reports

1. The consultant shall prepare the documents in electronic format (WORD and PDF) in the language versions specified as follows:
 - a. Inception report - English and French
 - b. Draft revised Directive – English, French and Portuguese.
 - c. Final revised Directive – English, French and Portuguese.
2. The Initial and draft final reports will be presented to ECOWAS Member States experts for validation and must include the observations made until they have been deemed satisfactory. The inception report will be validated by the ECOWAS Commission
3. To facilitate the validation session, the consultant shall prepare workshop slides summarising the contents of the reports in English, French and Portuguese.

4. Consultant And ECOWAS Obligations

4.1. Consultant Obligations

- a. All the resources required to conduct the study shall be borne by the Consultant. This should therefore be factored in the bid preparation.
- b. The Consultant shall bear full responsibility for collecting data from ECOWAS Member States, ECOWAS Institutions and other stakeholders, and any liabilities that may be involved.
- c. The Consultant shall undertake to check the coherence of data and information collected as part of the execution of the mandate.
- d. The Consultant shall be required to comply with professional secrecy during and after the mission and keep an inventory of all documents produced and those placed at their disposal.
- e. In the methodology for the execution of the mission, the Consultant shall prepare a work plan taking into account the implementation timeline set out in section 3.
- f. The implementation timeline provided in 3.4 is indicative. It is assumed that there is possibility for some of the activities in the scope of work to be carried out concurrently.

Consultants' proposals shall therefore be assessed by their proposals to optimise the delivery.

- g. The Consultant will be expected to facilitate workshops for the validation of the deliverables. The workshops will be held physically in a city within the ECOWAS region and the expenses associated with the consultant's participation must be factored in the bid preparation.

4.2. ECOWAS Obligations

- a. The ECOWAS Commission shall provide the Consultant with all the useful documents and procedures at its disposal necessary for the execution of this assignment.
- b. ECOWAS shall validate the work methodology and monitor the proper execution of the assignment.
- c. ECOWAS shall also be responsible for organising a workshop with Member States experts to validate the deliverables and accept the conclusions of the work.

5. Consultant Qualifications and Experience

5.1. Qualifications and Skills

- Possess at least a Bachelors or Master's Degree in Law, ICT Law, International Law, or a related legal field relevant to the assignment.
- Additional qualifications or training relevant to the assignment will be highly appreciated.
- Exhibit excellent skills in oral communication, report writing, presentations, and workshop facilitation.

5.2. Experience

- Possess at least seven (7) years of professional experience or equivalent demonstrable expertise in the field of cybercrime as relevant to this assignment.
- Demonstrate a proven track record in developing and revising legal and regulatory frameworks for international or regional organisations. This should include examples of successful projects, publications, or contributions to significant legal reforms.
- Exhibit knowledge of the legal instruments of sub-regional, continental and international organisations to which ECOWAS Member States are parties, in the field of cybersecurity, cybercrime, protection of personal data, privacy laws and cross border data sharing frameworks.
- All experience must be substantiated by certificates of good execution, contracts or equivalent documentation.

5.3. Language

- The Consultant must demonstrate proficiency in at least more than one official languages of ECOWAS (English, French and Portuguese). Proficiency in a third language is an added advantage.
- The consultant (either individually or as a team) has the ability to work and review the relevant legal texts in the official languages of ECOWAS (English, French and Portuguese).
- The use of language experts for translation can be an option.

Note: Applicants must provide signed CVs (with references), diploma certificates, training certificates and mission/work certificates etc.