



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

TERMS OF REFERENCE (TOR)

DEVELOPMENT OF THE ECOWAS REGIONAL CYBERSECURITY AND CYBERCRIME STRATEGY (2027–2032)

1. BACKGROUND

The Economic Community of West African States (ECOWAS) adopted its first regional cybersecurity and cybercrime strategy in January 2021 to strengthen collective resilience, harmonise legal and policy frameworks, and enhance cross-border cooperation. Progress has been recorded across Member States, though unevenly, reflecting differences in institutional maturity, specialist skills, infrastructure reliability, resource constraints, and political cycles. These factors affect the pace and consistency of implementation and cooperation.

To address persistent gaps and evolving threats, ECOWAS has updated and introduced key instruments including:

- Supplementary Act A/SA.1/01/10 on Personal Data Protection, establishing a revised regional framework for privacy and data governance.
- Directive C/DIR 1/08/11 on fighting cybercrime, strengthened to improve operational effectiveness and judicial cooperation.
- Directive C/DIR.2/12/24 on Cyber/ICT Confidence Building Measures (CBMs) - providing guidance to promote stability, trust and responsible behaviour in cyberspace.

In partnership with the World Bank under the DTfA/WARDIP SOP-1 project, ECOWAS is working to expand broadband access, strengthen the digital economy, and lay the foundation for a single digital market in West Africa. The ECOWAS Commission is implementing programme components addressing *connectivity market integration, data market integration, and online market integration*. Achieving trust and resilience in cross-border services requires robust cyber governance, Computer Security Incident Response Team (CSIRT) capacity, and practical measures to protect Critical Infrastructure and Essential Services.

Meanwhile, the region's digital landscape is evolving, driven by emerging technologies such as Artificial Intelligence, 5G, and Cloud computing, alongside increasing internet penetration and the digitalisation of government and financial services. These developments present economic opportunities but also introduce substantial risks associated with cross-border impacts,

including regional cybercrime networks, shared infrastructure, and cross-border data flows. These risks include systemic risks such as PKI compromise; operational risks like phishing/SIM swap; sovereignty risks like cloud/vendor dependency, and societal risks such as deepfakes and any other risks identified during the consultation.

The 2021 Strategy provided a framework for coordinated development and joint initiatives, reflecting growing regional commitment to capacity building. However, persistent and emerging challenges highlight the need for a new, comprehensive regional cybersecurity strategy for 2027 – 2032. Priority areas include cross-border CSIRT cooperation, regional threat intelligence, harmonised legal response, pooled capacity building.

The new Strategy must balance ambition with feasibility, offering tiered pathways for Member States at different maturity levels, cost-effective measures that work despite constraints, and clear regional mechanisms for information-sharing, mutual assistance, and coordinated incident response. It should serve as a reference for national strategies and operational plans, while safeguarding rights and inclusion. Drawing on global best practices in cyber governance, incident response, and capacity building, the strategy will strengthen national mechanisms and foster cooperation. Beyond national benefits, the strategy will enable ECOWAS to:

- Enhance regional cybersecurity resilience and cooperation.
- Build collective capacity and protect cyberspace.
- Reinforce collective defence against cyber threats.
- Promote trusted digital transformation.
- Build confidence and security in the use of ICT, safeguard citizens, businesses, and critical infrastructure for a secure and inclusive digital future for West Africa.

2. PURPOSE

This Terms of Reference sets out the scope, deliverables, and requirements for a consultancy to develop guidance for developing a realistic, actionable, inclusive and costed ECOWAS Regional Cybersecurity and Cybercrime Strategy (2027 – 2032). The ECOWAS regional Cybersecurity and cybercrime strategy is structured to deliver distinct layers of purpose, including but not limited to the following:

a) Strategic Orientation (Direction)

The strategy provides a high-level roadmap by defining the region's long-term vision and ambitions. Key objectives include:

- Governance: Creating a unified regional cybersecurity governance framework for all Member States.

- Resilience and Trust: Identifying shared priorities to improve collective cyber resilience and foster trust in digital transformation efforts.
- Harmonization: Aligning legal and policy frameworks across the region while maintaining respect for individual national sovereignty and local contexts.

b) Implementation Guidance for Member States

This layer focuses on providing Member States with the necessary tools and pathways to execute the strategy locally:

- Capacity Building: Offering practical advice to enhance institutional capabilities and operational readiness.
- Maturity Models: Establishing tiered baselines and maturity models that account for the differing developmental stages of various countries
- Actionable Pathways: Pinpointing critical investments and clear steps for implementation at the national level.

c) Operational Coordination (At ECOWAS Level)

This layer outlines how ECOWAS and its Member States will function together in practice:

- Institutional Support: Clarifying the role of ECOWAS institutions in supporting Member States to bolster collective security.
- Cooperation Frameworks: Setting up systems for regional information sharing, mutual assistance, and joint incident response.
- Stakeholder Collaboration: Improving coordination between various stakeholders to effectively tackle cross-border cybercrime and security threats.

3. OBJECTIVES

Overall Objective:

Develop a costed, phased and measurable regional cybersecurity and cybercrime Strategy for 2027 – 2032 that enables ECOWAS to leverage its institutions and cooperation mechanisms to enhance the collective cyber resilience of the region.

Specific Objectives:

- Enhance regional cybersecurity resilience and collective defence through practical cooperation.
- Operationalise the adopted Directive on ECOWAS Confidence-Building Measures (CBMs) and cyber diplomacy to reduce misperception, improve information sharing, and enable mutual assistance among Member States.

- Address transnational cybercrime through workable legal enforcement and judicial cooperation tools, including digital evidence handling and cross border investigations aligned to good practice mechanisms and state obligations (e.g., Budapest Convention, Hanoi Convention).
- Protect critical infrastructure and essential services using minimum viable security baselines aligned with maturity tiers.
- Strengthen incident response and cyber governance capacity, including law enforcement, judicial cooperation, and digital forensics.
- Integrate emerging technology risk management (AI, 5G, Cloud) in a manner proportionate to local realities, such as available tools and skills etc. Prioritization will be determined by key criteria, including risk (focusing on high-impact threats), sector (targeting critical areas like ID and finance), and maturity level (aligning with country readiness), alongside other factors relevant to the local context Provide a Monitoring & Evaluation (M&E) framework with indicators, baselines, targets, and data sources.
- Outline suitable funding options, including Public Private Partnership (PPP) opportunities.
- Leverage regional mechanisms for coordinated incident response, crisis communication, and information-sharing (e.g., CSIRT-to-CSIRT cooperation, ISACs).

4. SCOPE OF WORK

The Consultant will undertake the following tasks:

- Assess existing ECOWAS cybersecurity strategies, policies, and action plans and report on the status of their implementation.
- Conduct a legal, policy, technical, and institutional gap analysis across Member States.
- Identify priority areas for regional support and intervention to help Member States achieve national objectives under existing ECOWAS instruments
- Develop strategic proposals and recommendations to strengthen regional cybersecurity and cybercrime cooperation based on identified gaps and emerging needs.
- Review relevant global and regional frameworks and benchmark against international standards and best practices.

- Engage stakeholders through consultations, workshops, and surveys to gather input and build consensus, including CSIRTs, law enforcement, judiciary, private sector and civil society.
- Draft the regional cybersecurity strategy, including vision, mission, objectives, strategic pillars, and action plans.
- Develop a five (5) year implementation roadmap with timelines, responsibilities, and resource requirements.
- Propose a monitoring and evaluation framework to track progress, outcomes and impact.

5. DELIVERABLES AND LANGUAGE REQUIREMENTS

5.1. DELIVERABLES

- a. **Inception Report** detailing the methodology and work plan.
- b. **Assessment Report:** The Consultant shall produce a standalone Implementation Gap Assessment covering all twelve ECOWAS member states. For each member state, the Assessment shall evaluate current status against the commitments established under the 2021–2026 strategy, identify what has and has not been achieved, and specify the conditions and actions required to advance to the next implementation threshold. The Assessment shall be conducted using a structured template applied consistently across all member states, with analytical depth calibrated to the severity of the implementation gap rather than uniform treatment of all twelve. The Assessment shall be completed prior to the drafting of the regional strategy document and shall serve as the primary evidentiary basis for the disaggregated action plan.
- c. **Deliverable 3 — Regional Cooperation Framework and Interim Governance Structure:** The Consultant shall design a regional cooperation framework that ensures continuity of regional functions throughout the strategy period. The framework shall establish a phased governance structure anchored in existing mechanisms — including the ISAC — that enables the region to operate effectively throughout the strategy period. The framework shall assign each major cooperation function, including information sharing, mutual assistance, and cross-border coordination, to the most appropriate institutional actor and shall define how responsibilities are assigned to each actor. The framework shall further define a tiered participation model that accounts for varying levels of member state institutional readiness, including entry conditions for member states that do not yet have a designated national cybersecurity authority, enacted legislation, or a functional CSIRT, so that the governance structure remains inclusive while remaining operational. The Consultant shall identify the minimum resourcing requirements — including Commission

Directorate capacity, ISAC operational requirements, and any external technical assistance needed — to sustain the transitional governance structure, ensuring that the framework is not merely defined on paper but is capable of functioning within realistic institutional and financial constraints.

- d. **Disaggregated Action Plan:** The Consultant shall produce a disaggregated action plan grounded in the Implementation Gap Assessment findings and structured around the pillars of the ITU Global Cybersecurity Index (GCI). The plan should employ a Clustered Implementation Approach, grouping Member States by their maturity levels to ensure that proposed actions are both realistic and impactful. Each cluster will be assigned specific implementation expectations tailored to their maturity level. For Member States in the lower tiers, the plan should prioritize "Foundational Pre-conditions" (e.g., establishing a National Cybersecurity Strategy or a legal framework) rather than advanced operational deliverables. For each Member State (within its assigned cluster), the Consultant shall identify two to three priority actions mapped to the GCI pillars.

The action plan shall specify for each priority action:

- The Responsible Institutional Actor: Identifying the primary domestic agency or entity.
- Indicative Timeline: Phased targets (Short-term vs. Medium-term) within the 2027–2032 strategy period.
- Indicative Cost Range: High-level budget estimates based on regional benchmarks.

e. Resource Mobilization & Financing

- Recognizing the limitations of direct Commission budget allocations, the Consultant shall:
- Map Funding Pathways: Identify existing or accessible external resources (e.g., donor programs, multilateral mechanisms, or bilateral partnerships)
- National Integration: Formulate actions so they can be seamlessly integrated into national development plans, allowing Member States to leverage their own resource-mobilization processes.
- Incentivizing Progress: Frame priority actions as catalysts for improving the Member State's global GCI ranking, thereby facilitating easier access to international technical and financial assistance.

f. Draft ECOWAS Cybersecurity & Cybercrime Strategy (2027 – 2032) including

- 1. A costed implementation Plan** (5-year roadmap with KPIs, sequenced actions, responsibilities and indicative budgets).

2. A Monitoring & Evaluation Framework (log frame, indicators, baselines, targets, data sources, reporting cycles etc).

g. Final Strategy package incorporating all feedback from validation workshops and integrating the implementation plan and M&E framework

The Consultant shall produce a financing plan showing what funding is, accessible, and what gap remains. The Commission and Member States will provide indicative financial information where available. Any financing maps developed at this stage would remain provisional and subject to revision as funding commitments, partner engagement, and implementation conditions become clearer.

5.2. LANGUAGE REQUIREMENTS

- Inception Report: English and French.
- All other deliverables: English, French, and Portuguese.
- Executive summaries should be prepared in all three languages.
- Translation and quality assurance are the responsibility of the Consultant

5.3. VALIDATION PROCESS

- The **Inception Report** shall be validated by the ECOWAS Commission.
- The **Draft Strategy** and **Draft Final Package** shall be presented to **Member State experts** (virtual and /or physical) for validation.
- Deliverables shall be revised based on consolidated feedback until deemed satisfactory by ECOWAS Commission and Member States.

5.4. COMMUNICATION

In addition to submitting deliverables, the consultant shall maintain regular communication with the ECOWAS Project Manager including periodic progress updates and coordination meetings.

5.5. INDICATIVE TIMELINE

Deliverables	
Contract signature	Week 0
Inception report (EN and FR)	Week 2
Validation of the report by the ECOWAS Commission	Week 3
Assessment report— First Draft	Week 6

Deliverables	
Assessment Report — Revised Draft (incorporating ECOWAS Commission feedback)	Week 8
Regional Cooperation Framework and Phased Governance Structure — 1st Draft	Week 9
Disaggregated Action Plan—1 st Draft	Week 10
Member state & stakeholder engagement (virtual)	Week 12
Regional Cooperation Framework and Action Plan — Revised Drafts (incorporating feedback)	Week 14
1 st Draft Strategy	Week 16
Validation Workshop Member States (virtual)	Week 18
2 nd Draft Strategy	Week 22
Assessment Report, Cooperation Framework, and Action Plan — Final Versions	Week 24
Final Validation Workshop Member States (physical)	Week 24
Final Strategy Package	Week 26

6. DURATION

The assignment shall be carried out within **Six (6) months**, including assessment, drafting, consultations, validation workshops, and finalisation.

7. CONSULTANTS AND ECOWAS OBLIGATIONS

7.1. CONSULTANT OBLIGATIONS OF THE CONSULTANCY FIRM

- a. All resources required to conduct the activity shall be borne by the firm. This should therefore be factored in the bid preparation.
- b. The Firm shall bear full responsibility for collecting data from ECOWAS Member States and Institutions/Agencies, and any liabilities that may be involved.
- c. The Firm shall verify the data and information collected as part of the execution of the assignment.
- d. In the methodology for carrying out the assignment, the firm shall prepare a work plan to take into account the implementation timetable set out.

- e. The firm shall be required to comply with professional secrecy during and after completion of the assignment and keep an inventory of all documents produced and those placed at their disposal.
- f. The firm will be expected to facilitate the Member States validation workshops.

7.2. ECOWAS OBLIGATIONS

- a. The ECOWAS Commission shall make available to the Firm all useful documentation and procedures at its disposal necessary for the execution of this assignment.
- b. The ECOWAS Commission shall be responsible for the introduction of the Firm to Member States.
- c. ECOWAS Commission shall validate the working methodology and monitor the proper execution of the assignment.
- d. ECOWAS shall organise a workshop with Member States' experts to validate the deliverables and accept the conclusions of the work.

8. CONSULTANTS PROFILE

8.1. QUALIFICATION AND EXPERIENCE OF THE CONSULTANT

This assignment requires a consulting firm with strong experience in cybersecurity, ICT policy and digital governance, and a thorough understanding of cybersecurity challenges and opportunities. The firm must demonstrate expertise in:

- Governance, legislation and cyber risk management.
- Protection of critical information infrastructures.
- Incident response and development of cybersecurity skills.

The consulting should have:

- At least 10 years of proven experience in cybersecurity, ICT policy, or digital governance.
- Demonstrated experience supporting national or regional institutions in developing cybersecurity or cybercrime strategies.
- A track record of similar assignments involving regional or multi-country assessments, legal and institutional gap analyses.
- Experience leading stakeholder consultations across multiple sectors and Member States.

- Adequate technical and administrative capacity to implement the assignment (evidenced by copies of contracts, certificates of satisfactory performance, etc.).

8.2. COMPOSITION AND QUALIFICATION OF KEY PERSONNEL

Given the multidisciplinary nature of the assignment, the consulting firm shall mobilise a highly qualified team capable of analysing ECOWAS specific needs and making appropriate recommendations for the development of the strategy.

The core team should include at minimum:

- Team Leader/ Project manager
- Senior Cybersecurity Strategy Expert.

8.2.1.K1. TEAM LEADER / PROJECT MANAGER

Role: Lead and coordinate the assignment; provide methodological guidance; draft and consolidate the Strategy; ensure quality assurance; serve as the primary interface with ECOWAS.

Qualifications:

- Master's degree in Cybersecurity, ICT Policy, Computer Science, or a related field.
- Minimum of 10 years' professional experience in national or regional cybersecurity policy development, strategic planning, and governance.
- Proven experience developing at least two national or regional cybersecurity strategies (experience in West Africa is an asset).
- Familiarity with ECOWAS and African Union cybersecurity frameworks, ITU Cybersecurity Index, and international best practices.
- Demonstrated ability to lead multidisciplinary teams and facilitate multi-country stakeholder consultations.
- Strong diplomatic communication and stakeholder engagement skills.

8.2.2.K2. SENIOR CYBERSECURITY STRATEGY EXPERT

Role: Oversee programme management, timelines, resources, budgeting, and risk tracking; ensure deliverable quality and coordination across experts; organise validation processes.

Qualifications:

- Master's degree in cybersecurity, ICT Management, Public Policy, or a related field.

- At least 10 years' experience managing complex, multi-country cybersecurity or digital projects.
- Minimum of 5 years' specific experience in cybersecurity.
- Prior experience working with government institutions in West Africa preferred.

8.3. LANGUAGE & REGIONAL REPRESENTATION:

- Each expert must be proficient in at least one ECOWAS official language (English, French, Portuguese).
- Proficiency in additional languages and the inclusion of ECOWAS nationals in the team are distinct advantages.

9. COORDINATION AND REPORTING

The Consultant will report to the ECOWAS Directorate of Digital Economy & Post (DDEP) and provide regular progress updates as agreed.

10. ETHICAL STANDARDS AND CONFIDENTIALITY

All data, assessments, and draft documents must be handled confidentially. The Consultant must adhere to ECOWAS data protection standards and international ethical norms.