ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Terms of Reference
Feasibility study for the establishment of an ECOWAS Regional Cybersecurity Coordination Centre

1. Background and Rationale

The Economic Community of West African States (ECOWAS), established by the Treaty of Lagos on 28 May 1975, is one of the five (5) Regional Economic Communities (RECs) of the African Union. This regional organisation for West Africa brings together fifteen (15) Member States (Benin, Burkina Faso, Cabo Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo).

The mission of ECOWAS is to promote cooperation and integration leading to the establishment of an Economic Union in West Africa in order to raise the standard of living of the people and ensure economic growth, promote good relations between Member States and contribute to the progress and development of the African continent. To achieve its objectives, the Community implements programmes, projects, and activities in all socio-economic fields including Agriculture, Energy Transport, Digital Economy, Trade, Peace, and Security, etc.

In the digital field, the ECOWAS Commission has embarked on major initiatives aimed at using Information and Communication Technology (ICT) for development. Indeed, ICTs have become an integral part of modern societies and are ubiquitous, continuously transforming lifestyles. The availability of ICTs and related services offer a number of benefits for society at large, and ICT applications, such as e-government, e-commerce, e-education, and e-health, are seen as catalysts for the socio-economic development. For example, the amount recorded for the economic value created in West Africa by mobile technologies and services in 2018 is USD 52 billion, or 8.7% of GDP. According to estimates, this amount is expected to reach nearly 70 billion (9.5% of GDP) in 2025.[1]

In addition, the liberalisation of the telecommunications/ICT sector has led to significant progress in the development of broadband infrastructure, which is the cornerstone of the

[1] GSMA Mobile Economy West Africa 2019 report

development of regional and international connectivity, and in turn the development of the Internet.

The internet penetration rate in West Africa has been on the rise, increasing from 47.44% as of 31 December 2019 to over 54% by the end of December 2021. This rate is well above the African average of 43.2%, but still lower than the world average of 67.9%. However, this penetration rate for West Africa is expected to grow with the rise of new technologies, the continued deployment of broadband, as well as the digital transformation initiated by Member States, and thus allowing ECOWAS citizens to benefit from increased access to high-speed Internet capacity through which ICT-related innovations can be harnessed for economic growth and social development at the regional level.

However, this increased connectivity, which is transforming our societies and economies, also exposes ECOWAS Member States to increasingly complex and sophisticated cyber risks causing enormous damage and financial loss. For instance:

- **Nigeria:** Kaspersky's 2023 released statistics related to the regional threat landscape in Africa highlight Nigeria's experience. During Q3 2023, Nigeria witnessed a 12% increase in phishing attack detections compared to Q2. Additionally, 28% of Industrial Control Systems (ICS) computers in Nigeria were targeted by attacks during the same period and furthermore 6% of Internet of Things (IoT) devices faced security breaches.
- **Ghana:** In 2022, following an attack on the Electricity Company of Ghana (ECG), customers of the country's largest electricity provider experienced power outages for several days due to the disruption of some systems.
- **Burkina Faso:** The Central Brigade for the Fight against Cybercrime (BCLCC) in Burkina Faso reported a financial loss of 1,400,000,000 CFA francs (approximately $US 2,327,346) due to cybercrime between May 2020 and June 2021.
- **Côte d'Ivoire:** The Platform for the Fight against Cybercrime of Côte d'Ivoire indicates a financial loss of 6,172,067,179 CFA francs (approximately $US 10,260,383) in 2020.

The level of cybersecurity maturity of most ECOWAS Member States remains low and could increase the challenges related to cybercrime. According to the International Telecommunication Union's (ITU) 2020 Global Cybersecurity Index (GCI) report measuring countries' commitment to cybersecurity, only four (4) ECOWAS Member States (Ghana, Nigeria, Benin, and Côte d'Ivoire) have an above-average index. However, the best country in the region, Ghana, is 4th in sub-Saharan Africa and 43rd in the world. It is therefore

imperative to have robust security measures in place to protect governments, businesses, critical infrastructure, sensitive data, and citizens in the region.

To address this issue, the ECOWAS Council of Ministers adopted *Directive C/DIR.1/01/2021 on the adoption of the regional cybersecurity and cybercrime strategy* in order to make the most of technological advances, improve the level of national and regional cybersecurity and cybercrime mechanisms, and develop cooperation and mutual assistance among Member States in the region. To support and promote this cooperation and mutual assistance between the Member States of the Community, the regional strategy requests the ECOWAS Commission, in its sub-objective 5.3, to explore with Member States the feasibility of creating, in the short or medium term, an ECOWAS Regional Cybersecurity Coordination Centre (hereafter "the Centre".
The feasibility study will determine how the Centre could organise, where possible, the pooling of resources and sharing of information between countries with a view to mitigating the harmful effects of cybersecurity incidents.

The establishment of an ECOWAS Regional Cybersecurity Coordination Centre would have several relevant benefits for the security of cyberspace, including:

- **Enhanced collaboration**: A regional coordination hub would enable better collaboration between key cybersecurity actors, such as the Computer Security Incident Response Team (CSIRT) and all stakeholders involved in strengthening cybersecurity and combating cybercrime. This would facilitate the exchange of information, the coordination of actions and the pooling of resources to deal with cyber threats.
- **Incident management**: A regional coordination centre could play a key role in the management of cyber security incidents. It could serve as a central point for the collection and analysis of data related to cyberattacks, allowing for a rapid and effective response. Such coordination would reduce response times and promote better protection of critical infrastructure at regional level.
- **Sharing expertise**: By bringing cybersecurity experts together in a regional hub, it would be possible to facilitate the sharing of knowledge and best practices. This would enable countries and organizations in the region to strengthen their cybersecurity skills and improve their ability to prevent, detect and respond to security incidents.
- **Awareness-raising and training:** The regional centre could also play an important role in raising awareness of cybersecurity and training relevant stakeholders. It could

support awareness-raising initiatives, organise trainings, and share educational resources to build digital security skills in the region.

- **Regulatory harmonisation:** A regional coordination centre could support the harmonisation of cybersecurity regulations and standards within ECOWAS and foster cross-border cooperation and simplify the compliance of regional actors with international best practices on cybersecurity and cybercrime.

The CSIRT Week and the ECOWAS Symposium on Cybersecurity held in 2023 recognised the importance of the creation of a Regional Cybersecurity Coordination Centre and recommended that a detailed feasibility study be conducted for a justified decision on the establishment of the centre by ECOWAS Bodies (Experts, Sectoral Ministers, Administration and Finance Committee, Council of Ministers/Assembly of Heads of State and Government).

This Terms of Reference (ToR) for the feasibility study aims to assess the establishment of a Regional Cybersecurity Coordination Centre within the Economic Community of West African States (ECOWAS) with a view to strengthening digital security and promoting regional cooperation in a context of growing cyber threats.

2. Objectives of the Study and Scope of Engagement

2.1. Overall Objective

The objective of this feasibility study is to assess the technical, economic, and operational feasibility of setting up a Regional Cybersecurity Coordination Centre for the ECOWAS region in order to coordinate efforts in the management of cyber incidents including prevention, detection and response to cyberattacks within ECOWAS. The Centre would also foster collaboration between member countries, the sharing of information on threats and the training of key actors.

2.2. Specific Objectives

The specific objectives will be to:

a. Benchmark similar projects/centres at the global level
b. Refine the scope of work of the Centre to minimize overlap and maximize synergies with other regional initiatives (e.g., UNECA's ACCRC, AUC, Smart Africa, AfricaCERT, etc.), in

order to focus on one or two demand-driven, specific value propositions that would bring the highest return on investment.

c. Assess organisational feasibility, i.e. consider whether relevant stakeholders, such as government agencies, private companies and other actors involved in Cybersecurity, are willing to cooperate and actively participate in the coordination centre.
d. Assess the infrastructure and technologies required to establish a Cyber Security Coordination Centre.
e. Analyse financial feasibility by assessing the costs associated with setting up and operating the centre, including initial investments, maintenance costs, and human resources required.
f. Review the legal and regulatory or policy considerations to be taken into account for the establishment and operation of the centre to ensure that the coordination centre is in compliance with legal requirements.
g. Assess the expected benefits of the Cybersecurity Coordination Centre, such as improved coordination among stakeholders, cyberattack prevention and awareness, as well as the associated potential risks.
h. Propose a fundraising strategy to cover the investment and operating costs of the centre.
i. Propose a governance structure for the Cyber Security Centre with procedures and decision-making mechanisms.
j. Implement indicators to monitor and evaluate the performance of the Cyber Security Centre
k. Establish a timetable for the establishment of the Cyber Security Centre, including the distribution of tasks and responsibilities between the various actors involved in the centre.
l. Make appropriate recommendations for the sustainability of the Centre.

3. Expected Deliverables and Implementation Timeline

3.1. Deliverables and documents to be produced.

The consultancy firm (or firm) must produce the following deliverables:

1. Initial report detailing the proposed detailed methodology (outlining how each objective will be met, including research methods, stakeholder engagement strategies, and data analysis techniques), timeline, and resources for the completion of the feasibility study.

2. Preliminary report outlining the existing and expected regional cybersecurity initiatives and associated potential synergies, the CSIRT ecosystem in the ECOWAS region as well as cybersecurity and cybercrime stakeholders, key success factors and challenges for the establishment and operation of a regional cybersecurity centre.
3. Draft final report of the feasibility study containing technical requirements, costs, legal/regulatory/policy considerations, and mechanisms to sustain the establishment and operation of the centre.
4. Final report taking into account the comments from the workshop to validate the draft report.

The Consultancy will prepare the documents in electronic format (WORD and PDF) in the language versions specified as follows:

1. Initial Report – English or French
2. Preliminary Report – English and French and Portuguese.
3. Draft Final Report – English and French and Portuguese.
4. Final Report – English, French and Portuguese.

The preliminary report and the draft final report will be presented to the experts of ECOWAS Member States for validation and these reports should include the comments made until they are deemed satisfactory. The initial report will be validated by the ECOWAS Commission.

3.2. Timeline for the implementation of the feasibility study

The duration of the mission should not exceed twenty (20) weeks, and will be carried out according to the indicative schedule below:

Timeline	Deliverables
Contract signing + 2 weeks.	Initial report detailing the proposed methodology, timeline, and resources for the completion of the feasibility study.
Contract signing + 4 weeks	Validation of the report by the ECOWAS Commission
Contract signing + 12 weeks	Preliminary report containing the CSIRT ecosystem in the ECOWAS region as well as cybersecurity and cybercrime stakeholders, key success factors and challenges for the establishment and operation of a regional cybersecurity hub

Timeline	Deliverables
Contract signing + 16 weeks	Validation (virtual) of the preliminary report by Member States
Contract signing + 20 weeks	Draft Final Report of the Feasibility Study containing the technical requirements, costs, legal/regulatory/policy considerations, and mechanisms for sustainability for the establishment and operation of the Centre
Contract signing + 22 weeks	Validation of the draft final report by Member States
Contract signing + 24 weeks	Submission of the final report (in the 3 official languages of ECOWAS) taking into account observations from the validation of the draft report.

In addition to submitting deliverables, the Consultant will communicate regularly with the ECOWAS Project Manager.

4. CONSULTANTS AND ECOWAS OBLIGATIONS

4.1. Consultant Obligations of the consultancy firm

a. All resources required to conduct the study 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 in paragraph 3.2.
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.

4.2. 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.

5. PROFILE OF THE CONSULTANCY FIRM

5.1. Qualifications of the Firm/Consultants

This assignment requires firms with strong experience in the digital sector and a good understanding of the challenges and opportunities inherent in the field of cybersecurity, as well as demonstrable knowledge and experience in the following areas: governance, legislation, risk management, protection of critical information infrastructures, incident response and development of cybersecurity skills.

The realisation of cybersecurity policy projects, the development of cybersecurity architecture documents, will be an important criterion in the choice of the firm. As such, the firms concerned will have to justify at least five (5) years of experience in consultancy. They will also need to have worked on at least one (1) cybersecurity project in the last five (05) years.

5.2. Team Qualification

The firm will propose a core team comprising at a minimum:

- One (1) Team Leader/Project Manager
- A Cyber Threat Analysis and Incident Management Specialist
- A Cyber Security Policy and Governance Specialist
- A cybersecurity lawyer (regulatory expert)

The team of consultants should have the capacity to analyse the specific needs of ECOWAS and make appropriate recommendations for the establishment of an effective Centre.

Project Manager

One (1) Project Manager with experience in managing cybersecurity projects and knowledge of global best practices in cybersecurity policy development and who will be responsible for

overseeing the entire feasibility study. He/she will have to coordinate with all experts, manage deadlines, allocate resources, and ensure the proper execution of the project. He/she will be responsible for analysing the viability of the establishment of the Centre and will have previous experience of working with government institutions including in the ECOWAS region. He/she must have at least a Master's degree and 10 years of experience in the digital economy sector. In addition, he/she must have at least five (5) years of relevant professional experience in the field of cybersecurity.

Cybersecurity Lawyer

He/she should have proven knowledge and experience in the analysis of legal and regulatory frameworks in developing countries; knowledge of relevant legal and regulatory requirements, such as data protection regulations, of the West African legal system is highly desired. He/she will need to have a good understanding of the requirements and knowledge of the legal implications of cybersecurity policies and measures, including cybersecurity strategies and the establishment of CSIRTs; and will be responsible for identifying legal, regulatory or policy considerations that need to be taken into account when establishing and operating the Centre. He/she must have at least a master's degree in law and a minimum of 8 years of experience in the digital economy sector, including 5 years in cybersecurity and cybercrime aspects.

Cybersecurity Policy & Governance Specialist

The ideal candidate for this position must have in-depth knowledge of IT security best practices, current cyber threats, and cyber-attack prevention strategies. He/She should have a mastery of cybersecurity policies and standards at national, regional, and international levels, and an ability to conduct in-depth cybersecurity risk analyses and identify potential vulnerabilities. Experience in responding to cybersecurity incidents is preferred, with a focus on establishing and managing CSIRTs. Additionally, He/She should have at least a master's degree in Computer Science, Software Engineering, Cybersecurity/information security or other relevant fields and have at least 5 years of experience in cybersecurity policy and governance. Certifications or training on cybersecurity topics would be an advantage.

Cyber Threat Analysis and Incident Management Specialist

The ideal candidate for this position must have in-depth knowledge of cyber threats and attack techniques, risk analysis skills in identifying critical assets, vulnerabilities, and

determining the potential impacts of an attack, and in-depth knowledge of the fundamentals of IT security, network protocols, operating systems, and application security. He/She should have at least a Master's degree (or equivalent) in Computer Security, Software Engineering or a similar discipline from a recognised university and have at least 5 years of experience in the field of cybersecurity with a focus in CSIRT management. Certifications or training on cybersecurity topics would be an advantage.

Each member of the team must have a good command of at least one of the official languages of ECOWAS (English, French and Portuguese); A good knowledge of one of the other two will be an advantage.