Inter-governmental Authority on Development

TERMS OF REFERENCE

CONSULTANCY SERVICES TO DEVOLOP AN IMPLEMENTATION PLAN TO ESTABLISH A REGIONAL INFORMATION SHARING AND ANALYSIS CENTER (ISAC) FOR THE INTERGOVERNMENTAL AUTHORITY ON DEVELOPMENT (IGAD)

Project: Eastern Africa Regional Digital Integration Project
Contract type: Consultancy Services (firm or consortium)
Estimated Duration: 20 weeks
Location: Remote with field missions as needed.

A. BACKGROUND

Eastern Africa Regional Digital Integration Project

The Eastern Africa Regional Digital Integration Project (EARDIP), financed by the World Bank, aims to promote the expansion of an integrated digital market across Eastern Africa by increasing cross-border broadband connectivity, data flows and digital trade in the region. The Phase I development objective of the SOP is to advance digital market integration in the Eastern Africa region by increasing affordable access to regional broadband connectivity and strengthening the enabling environment for cross-border digital services.
EARDIP supporting two RECs, namely Eastern Africa Community (EAC) and Intergovernmental Authority on Development (IGAD) to be conduits of digital integration in the Eastern Africa region including the Horn of Africa region.

The Project under IGAD is structured in four components:

Component 1: Connectivity Market Development and Integration

Sub-component 1.3: Enabling legal, regulatory, and institutional ICT environment.
The aim of this sub-component is to support the harmonization of cross-border telecommunication infrastructure and services in the EAC and IGAD member states, the project will finance a set of legal, regulatory, and technical assistance activities and capacity building programs.

Component 2: Data Market Development and Integration

Sub-component 2.1: Cybersecurity frameworks, infrastructure, and capacity
This subcomponent aims to strengthen and harmonize cybersecurity frameworks across the IGAD member states to enhance the security of the cross-border data flows. It will comprise financing for legal and technical assistance as well as capacity building for managing cybersecurity risks, conducting awareness campaigns about cyber security at the regional level, and acquiring services and equipment for the creation of a regional incident response, information sharing, and cybersecurity coordination platform.

Sub-component 2.2: Data exchange, governance and protection

This sub-component would focus on safeguarding personal data, promoting trust and enabling cross-border data flows. Activities under this subcomponent will focus on enhancing the regional enabling environment and institutions required to integrate the data market through the harmonization of data protection regulation.

Component 3: Online Market Development and integration

Sub-component 3.1: Digital cross-border trade, payment and service enablers.

To promote trade in services and e-commerce across the region, this subcomponent would support the development of such a strategy for IGAD, preparing the ground for AfCFTA's E-Commerce protocol negotiations. The activities under this sub-component will support the establishment of region-wide rules on online markets by promoting the harmonization of laws and regulations in a series of policy areas essential to digital markets integration. Policy areas covered by this subcomponent will focus on enabling remote transactions, such as the regulatory framework for e-signature, online intermediaries and interoperability of payments.

Component 4: Project Management and Implementation Support

This component will finance technical assistance and capacity support for project implementation and the cost of setting up and operating costs of the Project Implementation Unit (PIU) within the Division of Economic Cooperation and Regional Integration of IGAD.

EARDIP builds on IGAD's Regional Infrastructure Master Plan (IRIMP, 2017-2021), supported by the African Development Bank. The main goal of the IGAD Regional Infrastructure Master Plan (IRIMP), the ICT sector is to develop smart and integrated ICT infrastructure. The main specific objectives are to develop harmonized policy and regulatory frameworks; promote the development of ICT services and e-applications, fast track the development of physical infrastructure, create safe cyber space, build capacity of the human resources and the related institutions.

In general, the situational analysis of the ICT sector in the region revealed that the sector is facing many challenges: (i) Access: lack of coherent, harmonized and holistic policies/strategies and action plans which impede infrastructure development as well as conducive legal and regulatory framework, (ii) Affordability: unaffordable access costs particularly for the poor living in rural areas, hence the increase of digital divide; (iii) Digital skills/literacy: poor digital training offers, lack of required equipment, etc.; (iv) Content relevancy: inadequacy of the offered content in relation to the needs of end users; and (v) Online safety: increased risks in terms of cybersecurity and lack of data and consumer protection frameworks and laws.

This consultancy will be implemented under component two of the EARDIP project, sub-component 2.1. IGAD in collaboration and support from the World Bank is intending to hire a consultancy firm to undertake this consultancy and support the decision makers with an

implementation plan to inform the establishment of a Regional Information Sharing and Analysis Centre (ISAC) for IGAD to support in gathering information on cyber threats as well as allow a two-way sharing of information between the private and public sector about root causes, incidents and threats and in addition sharing of experience, knowledge and analysis.

B. OBJECTIVE

IGAD Secretariat is seeking the services of a qualified firm to develop a plan to establish a regional Information Sharing and Analysis Center (ISAC) within the IGAD membership ("the Plan"). The Plan will reflect the needs, requirements and objectives of the region and will detail the service framework the regional ISAC should provide, its target audience and constituency, and necessary resources. The Plan should also include a step-by-step roadmap for establishing the regional ISAC, as well as relevant draft procurement documents. The Consultant will incorporate widely accepted Good Practices to enable the regional ISAC established through the Plan to participate in international cooperation initiatives and fora. The consultant will also provide recommendations to facilitate cooperation with other regional organisations in the area.

The scope of services, consulting team profiles, reporting requirements and other particulars of the assignment are detailed below.

C. SCOPE OF WORK

The Consultant is expected to carry out the following tasks:

- **Task 1 Prepare for on-site assessment**: The consultant will conduct studies and analysis of the regional current incident response and information sharing capabilities as well as the broader cybersecurity status of IGAD members. Relevant data and documents can be requested IGAD and member states, or consulted through desk research if available. This task includes the preparation of a list of relevant stakeholders to be interviewed during the consultation workshops.
- **Task 2 Conduct consultation workshops with relevant national and regional stakeholders:** the Consultant will hold a series of interactions and discussions with relevant stakeholders to assess the level of readiness for the creation of a regional ISAC. In this activity the consultant will conduct interviews, ask about the needs, goals to be achieved, possible agreements of information sharing, and discuss existing gaps and possible remediations. This task will inform task 3 and 4.
- **Task 3 Redact Readiness Assessment Report**: The consultant will prepare a report based on the information collected in Task 1 and 2. The report will provide an overview of the existing incident response and information sharing capabilities in the region, outline preliminary requirements (e.g., mandate, governance, high-level roadmap, budget) for the regional ISAC establishment plan, and provide insights on the broader cybersecurity context. This report shall include among others:
    - Brief review of existing information sharing and incident response capabilities
    - Goals and foundation
    - Preliminary Mandate
    - Governance Structure
    - Requirement for ISAC hosting organization
    - High-level roadmap and budget

    - High-level requirements for the Design Stage
    - Recommendations to facilitate cooperation with other entities in the region
- **Task 4 Redact ISAC Establishment Plan**: The consultant will develop a comprehensive plan that defines the services, target audience, necessary resources, and other relevant elements for establishing the regional ISAC. The consultant will also provide a step-by-step roadmap for implementing the plan. The Plan shall include among others:
    - Detailed Mandate
    - Vision, mission and objectives
    - Governance mechanisms
    - Information exchange policy
    - Legal structure and agreements
    - Business model
    - Service offering and operating model
    - Processes and Workflows Plan
    - Mechanisms and tools to collect and disseminate data
    - ICT plan
    - Facilities plan
    - Human resources plan
    - Detailed roadmap, timeline, resources and requirements for the Implementation Stage
    - Bidding documents to contract consultants for implementing the plan (e.g., RFP)
- **Task 5 Reporting to Project Manager**: The consultant will report regularly with the project manager and provide Status Update Reports, presentations, and other forms of communication as required.
- **Task 6 Other Applicable Tasks**: The consultant will carry out any additional tasks requested by the project manager within the scope of the deliverables outlined in this ToR.

All the activities and deliverables mentioned in this ToR shall be completed in conformity with the main internationally recognized standards and good practices. Annex B reports an indicative list of resources

D. EXPECTED DELIVERABLES & SCHEDULE OF COMPLETION

The Consultant is expected to complete the assignment in full within xx weeks, and to submit the following deliverables, based on the indicative timelines and payment schedule detailed below:

S/No	Milestone/deliverable	Timeline	Indicative payment schedule
D1.	**Inception report**, detailing how the assignment will be delivered, as per task 1	Within 1 week of contract signing.	10%
D2.	**Consultation workshop** with national and regional stakeholders, as per task 2	Within 5 weeks	
D3	**Readiness assessment report**., as per task 3	Within 10 weeks	50%
D4.	**ISAC establishment plan**, as per task 4	Within 14 weeks	

D5.	**ToR for ISAC establishment and Bidding documentation**, as per Task 4	Within 16 weeks	
D6.	**Final report**	Within 20 weeks	100%
D7.	**Short status update**	Every Three Weeks	

E. CONTRACTING, REPORTING AND VALIDATION PROCEEDURE

The Consultant will be contracted by IGAD, responsible for payment and approval of deliverables. All deliverables should be submitted to the IGAD Coordinator. Written deliverables should be submitted electronically in PDF and editable Word format efficient collaboration, comments, and edits with team members and reviewers.

The Consultant will collaborate on a day-to-day basis with the assigned IGAD Specialists, who may vary over time, and with the assigned focal points at the WB.

F. CLIENT'S RESPONSIBILITIES

IGAD, shall, to the best of their ability, provide the following:

- Background data and literature not readily available but considered relevant for accomplishing or informing the assignment and completing identified tasks at their immediate disposal.
- Access to key officials within the relevant Regulators/Ministries/Agencies/departments and other relevant official entities, as applicable.
- Cooperation with organizations, whose activities and programs are deemed relevant to the assignment and require an effort beyond what is reasonably attainable by the consultant.

G. LOCATION

Remote with field missions required.

H. KNOWLEDGE TRANSFER

Knowledge transfer is an integral part of this assignment and should be integrated into the consultant's methodology and technical proposal, assuring that the beneficiaries gain the capability to leverage and mobilize key elements of the assignment. For this purpose, the recommendations and analysis should be characterized by specificity, precision, and accompanied by concrete examples and an actionable, programmatic, and comprehensive roadmap to ensure practicality.

I. STAKEHOLDER CONSULTATION

As part of the project deliverables, the consultant will develop a consultation methodology that should be clearly specified to encompass a diverse range of stakeholders and topics. This methodology is essential for enabling a nuanced approach to adapting global good practices within

the region. It should proactively include various stakeholders, including civil society representatives at multiple phases, ensuring the creation of an inclusive and multifaceted analysis and recommendations.

An emphasis will be placed on the necessity of conducting simultaneous consultations involving multiple stakeholders. Additionally, it is advisable to conduct consultations, workshops, or a combination thereof before each deliverable and sub-deliverable. This approach ensures comprehensive representation and alignment with project goals.

The overarching goal is to facilitate a more comprehensive understanding of the ecosystem and the dynamics among various stakeholders. The outcomes shall be documented and shared with IGAD and WB.

J. REQUIRED EXPERIENCE: FIRM & CORE TEAM

The firm selected will need to demonstrate:

- Having strong skills and experience in cybersecurity and Information and Communication Technologies (ICT), particularly in the following areas: incident response, information sharing, cyber threat intelligence, digital forensics, with at least 5 years of relevant experience.
- At least 2 project references in the of Integrating and customization of ISAC/ISOC/CSIRT/CERT/CIRT/SOC Tools; Developing policies and procedures related to ISAC/ISOC/CSIRT/CERT/CIRT/SOC operations (operational workflows, SOPs, information sharing and incident management processes, service level management frameworks, among others); Setting up ISAC or Cybersecurity Operation center tools; or similar.
- Extensive knowledge of cybersecurity policy, strategy and operations in a government context.
- Demonstrating an understanding of relevant frameworks, methodologies, and best practices in cybersecurity.
- Prior experience working with the public sector is preferred.
- Experience in a developing country context, in particular in the IGAD context, is considered an advantage.

The firm shall propose a core team comprising of at minimum (1) Team Leader, (1) Information Sharing/Incident Response specialists, (1) Cybersecurity Governance and Risk Management specialist, and (1) legal and policy expert, plus any additional support staff deemed necessary to deliver the assignment. All team members must be fluent in English.

The consulting firm must provide a staffing plan with names, roles, and CVs for the core project team as part of the proposal.

Key Position	Experience	Qualifications
(1) Team Leader, or equivalent	• Minimum 7 years of experience in Cybersecurity program or project management experience specifically information sharing, incident response, cyberthreat intelligence and digital forensic. • Proven experience in managing and implementing ISAC/CIRT/CERT/CSIRT/SOC related projects in developing countries would be an advantage • Relevant certifications such as CISSP, CISM, or GCIH and internationally recognized SOC auditor certification	Master's degree in computer science, Cybersecurity, Science/Technology and/or other relevant fields.
(1) Information Sharing and Incident Response Specialist	• At least 5 years of experience in cybersecurity incident response, with a focus on establishing and managing ISAC/CIRTs • In-depth knowledge of IR and CIRT establishment frameworks and methodologies, such as FIRST service framework, NIST SP 800-61, ISO/IEC 27035, SANS Incident Handling Guidelines, and their application to building and operating effective CIRTs. • Proven ability to design and implement information sharing policies, procedures, and workflows, and to train and mentor ISAC members on information sharing and incident response best practices. • Relevant certifications, such as Certified Information Systems Security Professional (CISSP), GIAC Certified Incident Handler (GCIH), or EC-Council Certified Incident Handler (ECIH).	Master's degree in Cybersecurity/Information Security, Business/Public Administration, Economics, Development Studies, Commerce, Science/Technology, or other relevant fields.
(1) Governance and Risk Management Specialist	• At least 5 years of experience in risk management and CIIP, preferably at the national level. • In-depth knowledge of risk management and CIIP frameworks, such as NIST SP 800-53, ISO/IEC 27001, and their application to CII protection processes. • Relevant certifications, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or Certified Critical	Master's degree in Cybersecurity/Information Security, Business/Public Administration, Economics, Development Studies, Commerce, Science/Technology, or other relevant fields.

	Infrastructure Protection Professional (CCIPP),	
Legal and policy expert	• At least 5 year of experience in providing legal and policy advisory services in the field of cybersecurity. • Strong understanding of relevant laws, regulations, and industry standards governing information sharing and cybersecurity. • Experience in drafting and negotiating legal agreements, contracts, and policies related to information sharing and cybersecurity	Juris Doctor (J.D.) degree from an accredited law school with Specialization in cybersecurity law or related fields is preferred