TERMS OF REFERENCE

Intergovernmental Authority on Development (IGAD)
Harmonization of Cybersecurity Legal Frameworks in IGAD Member States

Project: Eastern Africa Regional Digital Integration Project SOP-II (P180931)
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.

Regarding cybersecurity, this master plan highlights the urgent need to review the current policies, legislations and regulations for the sector as whole including those related to cybersecurity and data protection. In addition to harmonization of policies and regulations there is a vital need for a regional cooperation framework since cybercrimes and threats have no border.

B. OBJECTIVE

IGAD is inviting qualified firms to conduct a comparative study in support of the harmonization of the cybersecurity legal framework (including, among others, cybersecurity, cybercrime, data protection, Critical Information Infrastructure Protection, digital identification, e-commerce, digital authentication, access to information, and related issues) of its Member States. This activity aims to strengthen the cybersecurity landscape within the region through a comprehensive review, identification of gaps, and formulation of actionable recommendations for both IGAD and its Member States.

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

C. SCOPE OF WORK

The consulting firm ("Consultant") will utilize a phased approach, drawing from regional and international standards and good practices. More specifically, the Consultant is expected to carry out the following tasks:

Task 1: Planning the assignment

- Develop a detailed plan to conduct the assignment including the proposed approach and methodology based on relevant good practices.
- Elaborate on requirements for data collection process including stakeholder engagement, data/document requests etc.
- Develop a consultation methodology. Clearly specify how this methodology will encompass a diverse range of stakeholders and topics, enabling a nuanced approach to adopting global best practices within the region. The methodology should proactively include various stakeholders, including civil society representatives at multiple phases, to ensure the creation of inclusive and multifaceted analysis and recommendations.

Task 2: Conduct a comparative study of cybersecurity legal frameworks of IGAD Member States

- Conduct a comprehensive and comparative review and analysis of the existing cybersecurity legal and regulatory frameworks within each IGAD Member State and in the region. This involves an examination of relevant laws, regulations, policies, and guidelines pertaining to cybersecurity, cybercrime, data protection, Critical Information Infrastructure Protection, digital identification, e-commerce, digital authentication, access to information, and related issues.
- Systematically identify and assess key gaps, weaknesses, and areas of improvement present in the current cybersecurity legal frameworks of IGAD Member States. This includes an in-depth analysis of legal ambiguities, inconsistencies, and inadequacies that may hinder the effectiveness of the cybersecurity landscape in the region. The analysis should include a comparative examination with specific examples of good practices, avoiding useless statements like 'this law is broad' or 'it lacks a provision." Focus on pinpointing exact deficiencies and outlining their practical consequences in terms of

regulatory enforcement, compliance, and market development.
- Conduct a consultation workshop with IGAD and its member states to build on the desk research and analysis and confirm scope of the legal challenges.

Task 3: Formulation of Actionable Recommendations

- Based on the findings from the review, develop a set of actionable and context-specific recommendations for both IGAD and its Member States. These recommendations should draw on both regional and international good practices in cybersecurity legislation. They should address identified gaps, promote consistency, and enhance the overall harmonization of cybersecurity legal and regulatory frameworks across IGAD Member States.
- Ensure that the proposed recommendations align with recognized international standards and best practices in cybersecurity. This involves considering frameworks such as the Budapest Convention on Cybercrime, the African Union Convention on Cyber Security and Personal Data Protection, and other relevant global conventions and guidelines.
- Ensure that recommendations are pragmatic in nature, developing them in alignment with factors such as urgency, complexity and challenges to enable IGAD and its member states to develop a comprehensive roadmap for action.

Task 4 Engage with relevant stakeholders as needed and facilitate a workshop to present the deliverables

- Facilitate engagement with relevant stakeholders, including government agencies, legal experts, cybersecurity professionals, and other entities involved in the development and implementation of cybersecurity laws to validate findings and recommendations. This may include conducting consultations, workshops, and roundtable discussions to gather diverse perspectives and ensure inclusivity in the harmonization process.
- Organize and conduct a workshop to present the final deliverables, including the comprehensive report, identified gaps, actionable recommendations, and any other relevant documentation. The workshop should provide an opportunity for interactive discussions, clarification of recommendations, and feedback from stakeholders.

D. EXPECTED DELIVERABLES & SCHEDULE OF COMPLETION

The Consultant is expected to complete the assignment in full within 24 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**, as per Task 1	Within 1 week of contract signing.	10%
D2.	**Comparative study of cybersecurity legal**	Within 12 weeks	50%

	frameworks of IGAD Member States, as per Task 2		
D3.	**Set of recommendations for IGAD and Set of recommendations for IGAD members**, as per Task 3	Within 17 weeks	40%
D4.	**Workshop to present the deliverables**, as per Task 4	Within 19 weeks	
D5.	**Final report**	Within 22 weeks	
D6.	**Short status update reports every 3 weeks**	Every 3 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 as well as with assignment focal points at the WB.

F. CLIENT'S RESPONSIBILITIES

IGAD, IGAD Member States, and WB 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 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 a 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:

- Extensive experience in the global legal aspects of Cybersecurity, cybercrime, data protection, Critical Information Infrastructure Protection, digital identification, e-commerce, digital authentication, access to information, and related issues, as well as practical implications, particularly in developing countries.
- A demonstrated track record of successfully completing similar assignments, with a focus on relevance and recent experience. This includes legal reviews, the development of legal frameworks, and formulating actionable recommendations to enhance cybersecurity legal frameworks based on recognized standards.
- Comprehensive knowledge of international and regional best practices in cybersecurity legislation and regulation, including but not limited to the Budapest Convention on Cybercrime, the African Union Convention on Cyber Security and Personal Data Protection, as well as other pertinent global conventions and guidelines.
- Knowledge of and practical experience with local and Regional legal systems and legal frameworks.
- Prior experience of working closely with public sector.
- Demonstrated familiarity with the Horn of Africa context.

The team composition is flexible, with a minimum requirement of at least one team leader and one team member. The firm may include additional team members as necessary to ensure the timely, accurate, and complete completion of the assignment, as per project requirements.

The consulting firm is required to provide a staffing plan as part of the proposal, which should include the names, roles, and CVs for the project team. Additionally, the team must identify the estimated number of days dedicated by each member to the project, specifying the periods and the tasks or responsibilities for which these days are allocated.

Team Leader or Equivalent: Minimum 10 years of experience in cybersecurity legal frameworks, with a proven track record of leading multiple similar assignments in the last three years and a Master's degree in Cybersecurity Law, International Law, Business/Public Administration, or a related field, or equivalent significant experience and a strong track record. Prior experience of leading at least two similar assignments.

Cybersecurity Legal Expertise: Minimum 7 years of experience in cybersecurity legal frameworks, with expertise in regional and international best practices. Supported at least three similar assignments. Possesses a Master's degree in Cybersecurity Law, International Law, Business/Public Administration, or a related field, or equivalent significant experience and a strong track record.

Regional Legal Expertise: Minimum 5 years of experience in cybersecurity legal frameworks with a specific focus on the regional context of IGAD Member States. Possesses a Master's degree in Cybersecurity Law, International Law, Business/Public Administration, or a related field, or equivalent significant experience and a strong track record.

Firms will undergo a holistic evaluation, with a focus on team composition that maximizes the timely, accurate, and complete completion of the assignment, aligning with project requirements.