Terms of Reference
for the position of Cybersecurity Expert - Tanzania

Project title: DEEP: Digital Economy, E-Commerce, E-Payment and Public E-Services Programme (EU-EAC DEEP)

1. Project description

The Multi-Donor Action "DEEP: Digital Economy, E-Commerce, E-Payment and Public E-Services Programme (EU-EAC DEEP) is part of the Pan-African "Safe Digital Boost for Africa" (SDBA) action in Sub-Saharan Africa.

The Action is jointly co-financed by the European Union, the Federal Ministry for Economic Cooperation and Development (BMZ), Ministry of Foreign Affairs France as well as Ministry of Foreign Affairs Estonia and implemented by Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) as part of the BMZ project "Support to East African Market Driven and People-Centered Integration (SEAMPEC)", Expertise France (EF) and the Estonian Centre for International Development (EstDev).

The duration of this Action is scheduled from July 2025 to March 2029 (48 months) with a total budget of 25.8 Mio. EUR.

The Action is the East African component of the SDBA Action Document and contributes to the Team Europe Initiatives "Supporting "African economic integration towards the African Continental Free Trade Area (AfCFTA) for eCommerce" and "Digital Economy and Society in Sub-Saharan" to provide comprehensive support for trade and digitalisation towards a sustainable setup of an African single digital market with a robust cybersecurity environment.

EU-EAC DEEP aims to foster the regional digital market of the East African Community (EAC) through cross-border E-Commerce and interoperable digital payment, support EAC regional digital transformation strategy by cyber-secure implementation for human-centered digital transformation and digital public infrastructure for EAC citizens.

The Overall Objective (Impact) of this Action is to accelerate digital trade and e-governance at continental, regional, and bilateral levels within a robust cybersecurity environment in the framework of an African single digital market.

The Specific Objectives (Outcomes) of this action are to:

1. Support the enhancement of the EAC operational readiness for the implementation of the digital transformation strategy. (Support to EAC Digital Transformation Strategy) – SO1
2. Enable, expand, improve and make more inclusive cross-border digital trade in East Africa. (eCommerce) – SO2
3. Improve cross-border ePayments and their interoperability in the EAC, including enabling and harmonising national payment systems. (ePayment) – SO3
4. Improve the organisational and technical enabling environment for eGovernance and enhance related cross-border interoperable service delivery. (eGovernance) – SO4

5. Enhance the development of regionally harmonised cybersecurity frameworks and the protection of critical infrastructure. (Cybersecurity) – SO5

The core project team is composed of the following:

- Team Leader (TL) based in Arusha (Tanzania)
- Field Project Officer (FPO) based in Kigali (Rwanda)
- Key Expert in Cybersecurity based in Arusha (Tanzania)
- Key Expert in eGovernment based in Kigali (Rwanda)

This core team is supported by a team based in Kigali (Rwanda) for financial and administrative and logistical aspects and a technical team based in EF HQ with two thematic project managers (Cybersecurity and eGovernance).

This EF project team will work within a Project Management Unit (PMU) lead by GIZ.

GIZ team leader will be responsible for overall DEEP coordination, while EF and ESTDEV team leaders will be both be deputies.

Short-term experts will contribute to the project on a punctual basis, depending on needs expressed by the beneficiaries and activities to be implemented.

2. Job description

a. General objective of the mission

Under the supervision of the EF Team Leader, he/she will be responsible for coordinating the Cybersecurity Component - Specific Objective 5 of the EU-EAC Deep. He/she will work in collaboration with the EF Team Leader and the EF Project Manager in Paris.

He/she will oversee implementation of the SO5 activities and ensure systematic coordination among implementing partners, in liaison with operational teams, HQ staff, and with the other SO experts.

The position implies a high degree of autonomy and interpersonal skills appropriate to working in an international and multicultural environment, as well as strong project management skills.

b. Description of the task to be assigned

Key Responsibilities (non-exhaustive list, subject to changes):

- Lead the overall planning, implementation, and monitoring of the SO5 across the EAC region;
- Propose the formulation of the work plan and ensure that the work plan developed is consistent with the project strategy;
- Coordinate with the SO5 implementing partner - ESTDEV;
- Design and develop activities under the technical perspective and ensure their quality;
- Coordinate and monitor the execution of SO5 annual work plan, budgets, timelines, and human resources, to ensure efficient and effective project implementation;
- Consolidate and coordinate the work of staff and experts, both hired by Expertise France and the other consortium agencies;
- Coordinate with Expertise France headquarters and other EU Member States implementing agencies, and other relevant stakeholders to ensure alignment with organizational strategies and policies;

- Coordinate SO5 evaluation and closure activities after the end of the implementation period;
- Participate in the project's steering committee meetings, and when relevant to the other SO activities (workshops, conferences and other meetings/events), showcasing project achievements and fostering collaboration with external partners.

Technical assistance and SO5 implementation:

- Ensure quality control and appropriate implementation of the activities related to the cybersecurity component for both implementing agencies;
- Provide technical assistance, training, and capacity building activities;
- Contribute to the development of context analyses and studies, steers their implementation and publication;
- Implement technical assistance missions in the following fields: Cybersecurity governance; National and Regional Cybersecurity and critical infrastructure strategies/policies; Regional, National Legal and regulatory frameworks related to cybersecurity; EU cybersecurity frameworks, tools and governance mechanisms; Technical trainings including table top and exercises; Awareness and sensitization campaign on digital hygiene and cybersecurity; CSIRT and SOC: Design, implementation, Management, Maturity assessment, etc;
- Draft the concept notes for each of the outputs under EF responsibility, clearly indicating the type of support, timeframe, content of the deliverable(s), and expert inputs (as and if appropriate);
- Draft the Terms of Reference related to EF short-term expertise needs, according to the timeline set in the planning of activities table and assist the team leader with their recruitment;
- Draft, in collaboration with other experts, mission and technical reports;
- Ensure the good coordination between the SO5 short-term experts and the quality of their deliverables;
- Liaise and coordinates with ESTDEV on the actions delivered by ESTDEV under the scope of SO5;
- Liaise and coordinates regularly with the eGovernance (SO4) expert (based in Rwanda) to ensure relevance of activities and cross-SO coherency;
- Participate in consultations and working groups with beneficiaries and partner organisations;
- Provide inputs to the project narrative reports.

Technical coordination and support to the implementation of activities to ensure the global coherence of the project

- Ensure the technical implementation of the SO5 outputs defining the activities to be done and the results to achieve
- Build up a database of short-term experts and contacts in the region;
- Ensures information flows between the SO5 activities (short-term experts from Expertise France and other implementing agencies) and the Project Management Unit;
- Ensure regular alignment and information sharing with the other SO2 and SO3 experts to identify synergies and avoid overlaps.

Cross-cutting missions:

- Support the MEAL responsible for pursuing monitoring and evaluation efforts related to SO5;
- Support visibility of Expertise France and Team Europe activities in the region;
- Ensure that the Team leader is informed on any critical issues that may jeopardize the project;
- Contribute to contractual, administrative, and financial management of SO5.

Any other task requested by Expertise France

c. Deliverables:

The Cybersecurity expert is responsible for ensuring the delivery of the SO5 outputs and for the production of the final outputs with which he/she is directly assigned.

In addition, the expert shall submit:

1. Terms of reference for the mobilization of short-term experts;
2. Inputs for the Narrative Progress Reports and the Final Report;
3. Ad-hoc meetings documentation and reports subject to adjustment at the end of the project.

All deliverables shall be submitted using the templates provided by Expertise France.

Table of deliverables

Periodic deliverables	
Deliverables	**Delivery frenquency**
Monthly report + timesheet	End of each month + 7 days
Minutes of strategic meetings with stakeholders, inputs on technical and steering committees meetings minutes	End of meeting + 7 days
Mission report	End of mission + 7 days
Annual detailed SO5 work plan	T0 + 4 weeks
Mapping of partners working on the theme/area	T0 + 4 months
Updated activities schedule	Every 3 months
Contribution to narrative reports for donor	T0 + 12 months x 1
Preparation and participation to team meetings	Each week
Preparation and participation to coordination and technical committees	TBC
Preparation and participation to steering committees	Once a year
Final deliverable	
Contribution to donor's final report	End of project + 1 month

T0 = date of notification of this contract

Additional deliverables may be requested and will be specified according to the specific needs of the project.

Validation of the deliverables presented by the designated expert will depend on their compliance with the requirements of the European Union and Expertise France.

d. Place, Duration and details of contract delivery

Place of performance: Position based in Arusha (Tanzania), full-time with regular field missions in Europe and in EAC countries and other locations depending on the project's needs.

Duration of the mission: One (1) year, renewable if performance is deemed satisfactory.

Period of the assignment: tentative January 2026 for 12 months (renewable up until the contractual end of the DEEP EAC project)

Type of contract: Fixed-term contract of employment with Expertise

e. Required profile

General and specific professional experience:

The ideal candidate has a Master's degree in IT, law, or a cybersecurity related field. Note that experienced that has adequate and demonstrable knowledge gained in praxis, in the area of cybersecurity, may also count towards meeting these criteria.

- At least 10 years of demonstrable experience in cybersecurity (cybersecurity and cybercrime issues according International and European conventions, directives and regulations), with broad political and intercultural competencies in international project implementation context;
- At least 5 years of experience in delivering cybersecurity related activities (research, practice or training), reports or training for international organisations or extensive experience gained in relevant institutions at the national level;
- At least 5 years of experience in working with Computer Emergency Response Team / Computer Incident Response Team CERT/CSIRT and or SOCs;
- At least 2 years of experience in developing regulatory and public policies and implementing information security policies;
- Experience in assessment of national legislation and regulation and comparison with best practices and international rules in order to enhance it;
- Experience in enhancement of capacity building and administrative reforms in Africa would be an asset;
- Experience in technical project management with planning, implementation processes which require coordination with stakeholders and logistics.

Ability to work in a public international environment:

- Good understanding of the European Commission and EU policies;
- Demonstrated ability to exchange with all institutional levels/ high-ranking dialogue partners;
- Working experience in/with the EAC partner countries would be an advantage;
- Fluent in spoken and written in English, strong reporting skills in the language;
- Knowledge of French would be an asset;
- Excellent communication skills, sense of diplomacy.

Good command of the organization of international activities :

- Capacity to organise successful activities in the framework of international cooperation projects;
- Computer proficiency including perfect command of office software;
- Organizational skills and thoroughness.

Additional specific requirements:

- Proficiency in working in a fast-paced, complex, dynamic, multicultural business environment is needed;
- Experience in EU funded projects is mandatory;
- Capacity to work under pressure;
- Good knowledge of the EAC partner States is a plus.

Please provide in English under the reference « Cybersecurity Expert – EU EAC DEEP » before 24/12/2025 through GEX platform:

- A resume in EU format stating credentials and references including company names, phone contacts and emails
- A cover letter

NB: Candidates interested in this opportunity are invited to submit their application as soon as possible, with Expertise France reserving the possibility of pre-screening before that date.