TERMS OF REFERENCE – FRAMEWORK CONTRACT

Individual Expertise Service Contract (CPS EI) – Cybersecurity Expert

EU-EAC DEEP Programme – Specific Objective 5 (SO5): Cybersecurity. Support to the EAC Cybersecurity Technical Working Group, regional CERT/CSIRT cooperation and regional cyber exercises

0. General information

Assignment name	Individual Expertise Service Contract (CPS EI) – Cybersecurity Expert - EU-EAC DEEP Programme
Type of the contract	Individual expertise service contract (CPS EI), concluded as a framework contract with an individual consultant and implemented through Purchase Orders
Country/location	Home-based, with missions in EAC Partner States or elsewhere as required. This information will be specified in each Purchase Order.
Total estimated number of days and contract duration	Up to 45 working days for the initial 24-month period. Up to 15 additional working days in case of renewal. Total maximum: 60 working days.

1. Background

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) initiative. It runs from July 2025 to June 2029 and covers the eight EAC Partner States: Burundi, the Democratic Republic of the Congo, Kenya, Rwanda, Somalia, South Sudan, Uganda and the United Republic of Tanzania.

Specific Objective 5 (Cybersecurity) aims to enable and enhance cybersecurity through regionally harmonised frameworks and policies for the protection of critical infrastructure, and capacity building. It is implemented by Expertise France, in close coordination with the EAC Secretariat, the EAC Cybersecurity Technical Working Group (CTWG) and the Partner States, and contributes to three outputs:

- Output 5.1: national and regional cybersecurity frameworks and critical infrastructure protection policies are developed and/or improved in line with international standards;
- Output 5.2: national, regional and international cooperation on cybersecurity and critical infrastructure protection is improved and promoted in the EAC States;
- Output 5.3: awareness of cybersecurity threats, cyber hygiene rules and individual responsibility is improved in the EAC States.

The first meeting of the EAC Regional CTWG (Nairobi, 28–30 July 2026) recognised the CTWG as the principal regional technical coordination platform for cybersecurity under the leadership of the EAC Secretariat. A draft SO5 workplan was presented, proposing in particular a mandate for the CTWG, an EAC CERT/CSIRT Cooperation Forum attached to the EAC Regional CERT, regional normative work (Regional Cybersecurity Strategy and Critical Information Infrastructure Protection (CIIP) policy) and

regional cyber exercises. The Partner States have also identified their cross-border cybersecurity needs, including threat intelligence sharing, incident response coordination, protection of critical information infrastructure, cyber exercises and capacity building.

Because these activities form a continuous programme of work over several years, building successively on the same CTWG process, workplan and operational instruments, the EU-EAC DEEP Programme wishes to secure the services of one individual expert through a framework contract. This ensures continuity of expertise, consistency of deliverables and timely mobilisation.

2. Purpose of the framework contract

The purpose of this framework contract is to make available to the EU-EAC DEEP Programme (SO5) the services of an individual consultant ("the Expert") providing technical expertise in cybersecurity, with a focus on regional cybersecurity coordination, CERT/CSIRT cooperation and cyber exercises. Services will be mobilised on an as-needed basis through Purchase Orders, as described in Section 5.

3. Objectives

Overall objective:

To provide technical cybersecurity expertise supporting the EAC Secretariat, the CTWG and the Partner States in strengthening regional cybersecurity governance, operational cooperation and preparedness, in line with the SO5 workplan.

Specific objectives – under this framework contract, the Expert may be requested to:

- Support the operationalisation of the CTWG and the prioritisation of the Partner States' cross-border cybersecurity needs into a validated workplan.
- Support regional normative work, in particular the Regional Cybersecurity Strategy and the CIIP policy, in line with international and European standards.
- Support the establishment of the EAC CERT/CSIRT Cooperation Forum and the development of common operational instruments for incident information sharing.
- Support the design, preparation and conduct of regional cyber drills and tabletop exercises, and their after-action reviews.
- Design and deliver technical training and contribute to capacity-building activities for cybersecurity authorities and CSIRTs/CERTs.

4. General scope of services

The services to be provided under this framework contract may include, without being limited to, the following types of activities. The precise tasks, deliverables, dates, location and number of days of each assignment will be defined in the Terms of Reference annexed to each Purchase Order.

4.1 Support to the EAC Cybersecurity Technical Working Group (Outputs 5.1 and 5.2)

- Preparation of a CTWG Terms of Reference proposal (mandate, membership, meeting rhythm, confidentiality and information-handling rules).
- Prioritisation and sequencing of the Partner States' needs into a Year-1 workplan, to be validated by the CTWG.
- Preparation and facilitation of CTWG meetings, virtual sessions and task teams (concept notes, agendas, presentations, minutes and action matrices).
- Technical inputs to the Regional Cybersecurity Strategy and CIIP policy (outlines, comparison of national frameworks, comment matrices, consolidated drafts).

4.2 Regional CERT/CSIRT cooperation and information sharing (Output 5.2)

- Support to the establishment of the EAC CERT/CSIRT Cooperation Forum (draft forum ToR, contact directory, information-handling rules).
- Development of common operational instruments: incident severity taxonomy, notification and escalation procedures, alert and request-for-assistance templates.
- Support to the design of a regional incident information-sharing and early warning mechanism, and to CSIRT readiness for international cooperation frameworks (e.g. FIRST).

4.3 Regional cyber drills and exercises (Output 5.2)

- Support to the design and facilitation of regional cyber exercises under EAC auspices (scenario, objectives, injects, evaluation framework, participant materials).
- Support to payment-system incident simulations and tabletop exercises, where relevant.
- After-action reviews and improvement plans feeding into the CTWG and the CERT/CSIRT Cooperation Forum.

4.4 Capacity building and remote support (Outputs 5.2 and 5.3)

- Design and delivery of technical training (incident handling, CSIRT operations, exercise facilitation), including training-of-trainers approaches.
- Home-based review of documentation, preparation of materials, reporting and follow-up coordination with the EAC Secretariat and Expertise France.

5. Implementation modalities: Purchase Orders

- Services are triggered exclusively through written Purchase Orders issued by Expertise France. The framework contract itself does not commit Expertise France to order any minimum number of days.
- Each Purchase Order will include specific Terms of Reference stating: the activity, the tasks, the expected deliverables, the number of working days, the dates and location, the reporting deadlines and the amount (number of days × daily fee set in the framework contract).
- The Expert shall confirm acceptance and availability within 7 working days of receipt of a draft Purchase Order.
- Only days actually ordered through a Purchase Order and performed, and whose deliverables have been approved, will be paid.
- The cumulative number of days ordered under all Purchase Orders may not exceed the maximum set in Section 8.
- No Purchase Order may run beyond the end date of the framework contract (and in any case beyond 31 March 2029), including its reporting period and the submission of deliverables.

6. Deliverables

The table below sets out the indicative deliverables and their distribution over the duration of the framework contract, in line with the SO5 workplan. The exact deliverables, deadlines and number of working days will be specified in each Purchase Order. Each mission will also give rise to a mission report, submitted within the deadline set in the Purchase Order.

Deliverable	Indicative timing
D1 – Technical inputs to the Terms of Reference and to the exercise package of the EAC Regional Cyber Drill (scenario, objectives, injects, evaluation framework, participant materials)	December 2026

D2 – After-action report of the regional cyber drill, with improvement plan	Within 15 working days of the exercise
D3 – CTWG follow-up workshop package (concept note, agenda, presentations) and workshop report with action matrix	December 2026 – January 2027
D4 – CTWG Terms of Reference proposal and prioritised Year-1 workplan, submitted for validation through EAC channels	Q1 2027
D5 – Technical inputs to the drafts of the Regional Cybersecurity Strategy and the CIIP policy (comment matrices, consolidated inputs)	Q2 2027
D6 – Draft Terms of Reference and operational instruments of the EAC CERT/CSIRT Cooperation Forum (contact directory, information-handling rules, incident severity taxonomy, alert and request-for-assistance templates)	Q3–Q4 2027
D7 – Training materials and training report for national CSIRTs/CERTs	Q4 2027 – Q1 2028
D8 – Exercise package and after-action report for a second regional exercise (tabletop or joint cyber exercise)	2028
D9 – Final report on the framework contract: results, lessons learned and recommendations	March 2029

All deliverables shall be in English, submitted to Expertise France and, where relevant, to the EAC Secretariat, and are subject to their approval.

7. Required qualifications and experience

Professional experience (50 points)

- At least 8 years of professional experience in cybersecurity (policy, operations, research or training).
- Demonstrated practical experience in support to regional cybersecurity coordination bodies, CSIRT/CERT operations and cooperation, and the design and facilitation of cyber exercises (cyber drills, tabletop exercises).
- Experience in capacity building and technical assistance in Africa, preferably in EAC Partner States, and in inter-agency, regional and international cooperation.
- Participation in similar EU-funded technical assistance projects would be an asset.

Qualifications and skills (40 points)

- At least Bachelor's degree in cybersecurity, information security, computer science, engineering, law, public policy or a related field, or equivalent work experience.
- Knowledge of international and European cybersecurity frameworks and standards (e.g. ENISA, NIS2, ISO/IEC 27000 series, NIST, Budapest and Malabo Conventions).
- Excellent written and spoken English; strong analytical, drafting, presentation and facilitation skills. Knowledge of French is an asset.
- Relevant professional certifications (e.g. CISSP, CISM, ISO/IEC 27001 Lead Implementer/Auditor, GIAC) would be an asset.

Additional requirements (10 points)

- Good understanding of EU policies and of the EAC institutional context.
- Demonstrated ability to engage with high-level institutional counterparts.
- Availability to be mobilised at short notice and to travel within the EAC region.

8. Duration, maximum volume and location

Type of contract	Individual expertise service contract (CPS EI), concluded as a framework contract with an individual consultant and implemented through Purchase Orders
Duration	The framework contract will enter into force on the date of signature by both parties for a duration of 24 months, and shall in any case end no later than 31 March 2029. It may be renewed once, by written amendment, subject to satisfactory performance, continued needs and availability of funds, for an additional period that shall in any case end no later than 31 March 2029.
Maximum volume	Up to 45 working days for the initial 24-month period. Up to 15 additional working days in case of renewal. Total maximum: 60 working days.
Maximum amount	Daily fee × maximum number of days (excluding VAT and reimbursable costs), within a ceiling of 39 000 EUR
Purchase Orders	No Purchase Order may be issued whose implementation period, including the reporting period and the submission of deliverables, extends beyond the end date of the framework contract, and in any case beyond 31 March 2029.
Location	Home-based, with missions in EAC Partner States or elsewhere as required. This information will be specified in each Purchase Order.
Travel	International and in-country travel, accommodation and per diem related to missions are covered by Expertise France in accordance with its applicable rules, and are not included in the daily fee.
Coordination	Expertise France SO5 Team Leader (or, once recruited, the SO5 Cybersecurity Key Expert), in coordination with the EAC Secretariat

9. Application documents

Interested candidates are invited to submit, in English:

- An updated CV, preferably in EU format, clearly indicating relevant cybersecurity experience and language proficiency.
- A short technical note (maximum 3 pages) presenting the candidate's understanding of the assignment, the proposed methodology and implementation approach, and availability.
- A financial proposal, as described in Section 10.

10. Financial proposal

The Expert is invited to submit a financial proposal stating a single all-inclusive daily fee in EUR, excluding VAT and excluding reimbursable costs (travel, accommodation and per diem, which are covered directly by Expertise France).

The daily fee shall cover all professional costs related to the implementation of the assignment (preparation, remote work, communication, equipment, insurance, etc.) and will remain fixed for the whole duration of the framework contract, including any renewal period.

11. Evaluation and selection

- Applications will first be assessed against the qualifications and experience set out in Section 7 (100 points) and the quality of the technical note.
- The technical and financial assessments will be weighted as follows: technical 70% / financial 30%.
- At least three shortlisted candidates may be invited to a negotiation on their technical and financial proposals.

12. Payment

Payment will be made by bank transfer per Purchase Order, upon satisfactory delivery and approval of the deliverables specified in that Purchase Order, on the basis of an invoice and a timesheet of days worked, in accordance with the terms of the framework contract.

13. Other provisions

- Confidentiality: all information obtained during the assignments, in particular on national cybersecurity arrangements, incidents and vulnerabilities, is strictly confidential and may not be disclosed without prior written consent.
- Intellectual property: all deliverables are the property of the EAC Secretariat / EU-EAC DEEP Programme.
- Independence: the Expert performs the services independently, as a service provider, and is responsible for his/her own tax and social security obligations.