

Terms of reference (ToR) for the procurement of services below the EU threshold

CONFIDENTIAL

Tender for E-Learning Course & Certification Bundles	Project number/ cost centre: G-012216-001 Tender number 10037211
---	---

0.	List of abbreviations	2
1.	Context.....	3
2.	Tasks to be performed by the contractor	4
3.	Costing requirements	Fehler! Textmarke nicht definiert.
4.	Inputs of GIZ or other actors.....	5
5.	Requirements on the format of the tender	Fehler! Textmarke nicht definiert.
6.	Outsourced processing of personal data	5
7.	Annexes	Fehler! Textmarke nicht definiert.

0. List of abbreviations

AG	Commissioning party
AN	Contractor
AVB	General Terms and Conditions of Contract for supplying services and work
ECOWAS	Economic Community of West African States
EU	European Union
FK	Expert
FKT	Expert days
FFO	Federal Foreign Office
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
KZFK	Short-term expert
ToRs	Terms of reference

1. Context

Background

Digital transformation brings with it both new opportunities and risks and vulnerabilities that must be taken into account and addressed by governments, organisations and citizens. Digital technologies are being used to attack critical infrastructure, disrupt digital services, commit cybercrime, increase surveillance, commit human rights violations and spread disinformation. This has serious negative consequences for individuals, the economy, society and public institutions, as well as for the overall stability of the global cyberspace.

The Federal Foreign Office (FFO) actively promotes international cybersecurity policies for a global, open, free, inclusive, stable and secure cyberspace. It works closely with relevant organisations, partners and stakeholders to increase cyber resilience, strengthen cybersecurity capabilities and improve the international cybersecurity architecture.

To support this endeavour, the Partnership for Strengthening Cybersecurity was launched in 2023 as one of Germany's instruments for providing technical capacity, fostering partnerships and raising public awareness. The programme is implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) on behalf of the FFO and, in part, by the European Union (EU). The aim is to contribute effectively to the global network of like-minded cooperation partners and to drive forward the development of cyber capabilities.

General objectives

The main objective of the Partnership for Strengthening Cybersecurity is to enhance the capabilities of selected bilateral and regional partners to prevent, mitigate and respond to cybersecurity threats. This includes fostering partnerships, raising public awareness and contributing to the global network of like-minded cooperation partners. The regional components focus on the Economic Community of West African States (ECOWAS), the Western Balkans, the African Union, and selected countries in Eastern Europe and the Southern Neighbourhood.

Rationale

The programme is designed to support partner countries in taking greater responsibility for their own cybersecurity. It aims to support the development of cybersecurity capabilities capable of addressing the evolving cyber threats to military and civilian critical infrastructure in Europe. This includes training specialists to implement international standards and best practices.

Specific objectives

The specific objective of the call for proposals is to support the ECOWAS Hackathon from 9–11 June in Accra, Ghana. The project 'Partnership for Strengthening Cybersecurity', commissioned by the FFO, supports the regional ECOWAS Hackathon by providing training opportunities for regional talent participating in the Hackathon. The aim of the Hackathon is to address the shortage of qualified specialists by identifying emerging West African talent and to contribute to strengthening the regional cyber ecosystem.

The initiative is embedded in German-EU cooperation on digital resilience in West Africa and supports the protection of critical infrastructure through improved detection, prevention and response capabilities. The winners of the hackathon will receive training and certification

from an internationally recognised cybersecurity service provider, enabling them to secure the networks and experience gained during the hackathon in the long term and to contribute certified expertise to the region.

By achieving these objectives, the program aims to improve overall cybersecurity in the ECOWAS region and contribute to the broader goals of the partnership to strengthen cybersecurity.

2. Tasks to be performed by the contractor

The contractor is responsible for providing the following services:

- **Provision of Training Bundles:** Provision of thirteen (13) individual Course & Certification Bundles (covering entry level to intermediary level courses, depending on the individual selection of the participants).
- **Course Assignment and Onboarding:** Facilitation of an independent course selection process for the 13 identified regional talents. Each participant must be granted individual autonomy to select a course aligned with their specialized interest (e.g., Web Application, Network Pentesting, Exploit Development, etc.).
- **Tailored Content:** Participants should be able to acquire the knowledge and certification required for one of the following roles: AI Red Teamer, Entry-Level and Experienced Penetration Tester, Web Assessor, Web Expert, Exploit Developer, Defense Analyst, Threat Hunter, and Incident Responder
- **Learning Platform Access Management:** Ensuring full, uninterrupted access to the digital learning platform for each participant for a continuous period of ninety (90) days per user. This must include comprehensive access to all relevant course videos, structured materials, documentation, and the accompanying hands-on virtual lab environments (minimum of 50 Proving Grounds Play labs per bundle), alongside bonus access to a Kali Linux operating system module.
- **Examination Administration:** Provision and administrative management of one (1) practical, performance-based certification exam attempt per participant. The exam must validate hands-on technical competence in realistic simulated environments rather than theoretical multiple-choice structures.
- **Trusted Certification:** Certification must be obtained through a fully live-monitored, practical examination which demonstrates the candidate's ability to cope with pressure and to engage in critical problem-solving under real-time conditions.
- **Technical Support:** Provision of technical platform support to the participants throughout their 90-day learning and examination windows to ensure smooth operation of the virtual lab environments.

Achievement of the milestones/bundles is subject to participants' cooperation (attendance of courses, completion of assignments, participation in examinations). The Contractor is obliged to duly deliver the agreed services (online platform, learning content, tutoring/support, examination administration). No warranty of outcome (e.g. participants passing exams/obtaining certifications) is given. Failure to complete or pass due to lack of participants' cooperation or performance does not constitute a breach by the Contractor.

Requirements for the training courses to be provided

Bidders must demonstrate that they can provide the following e-learning courses and certificates via an online platform:

- Certification for: AI Red Teamer, Entry-Level and Experienced Penetration Tester, Web Assessor, Web Expert, Exploit Developer, Defense Analyst, Threat Hunter, and Incident Responder
- Delivery mode: fully online, self-paced, exam administration included
- Language(s): English
- Number of access keys/seats: 13
- Availability period: 90 days validity per key after activation, activation at least two weeks after contract signature
- Data protection and information security: ability to comply with applicable data protection obligations, i.e. GDPR.

Offers that do not meet all above listed requirements will not be considered. Among all tenders that meet the requirements (pass/fail), the contract will be awarded to the lowest-priced offer (price-only evaluation).

Project Management and Reporting Requirements

- The contractor provides access to the courses and certifications and assumes the associated operating and administrative costs.

3. Inputs of GIZ or other actors

GIZ coordinates the necessary steps depending on the activation method: if activation is carried out using access keys, the contractor provides the access keys, GIZ receives them and distributes the keys to the 13 participants. If activation is via email addresses, the 13 participants collect their email addresses; GIZ coordinates the collection and forwards the addresses in a single batch to the contractor.

4. Outsourced processing of personal data

The performance of the contract may be associated with the processing of personal data by the contractor, such as (but not limited to) names and contact information. In such cases, the contractor shall act as an independent DATA CONTROLLER and must alone comply with ALL applicable data protection obligations, including those stemming from regional and local laws. The contractor shall process personal data only when a given goal cannot be reasonably attained without such data. The data protection principles such as lawfulness, data minimization, accuracy, purpose limitation, storage limitation, transparency, integrity and confidentiality, and accountability, as well as the numerous rights of the data subject must be paid due attention. The GIZ is NOT in any way responsible for such processing. Whenever the contractor executes the instructions of a partner to the GIZ with regard to such processing, the partner shall be the data controller. In such cases, the contractor shall comply with the laws and standards applicable to the partner. If the contractor is not subject to the GDPR and the applicable laws do not contain any explanation on the data protection

principles and rights mentioned here, the definitions and meanings provided by the GDPR (Regulation (EU) 2016/679) should be considered.