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

CONFIDENTIAL

Support to Development of an e-course on cybersecurity fundamentals for civil and municipal servants in Armenia	**Project number/ cost centre:** **22.9024.5-011.00**

0. List of abbreviations

AU	African Union
CERTs	Computer Emergency Response Teams
CV	Curriculum vitae
DC	Development cooperation
ECOWAS	Economic Community of West African States
EU	European Union
FFO	German Federal Foreign Office
GCI	Global Cybersecurity Index
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
ISMB	Information Systems Management Board
ISSA	Information Systems Agency of Armenia
ITU	International Telecommunication Union
ToR	Terms of reference

1. Context

Brief information on the project

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) is a federal enterprise and a global service provider of international cooperation for sustainable development. GIZ has more than 50 years of experience in a wide range of fields, from economic and employment promotion to energy and environmental issues to the promotion of peace and security. The diverse expertise of the federal enterprise GIZ is in demand around the globe - from the German Federal Government, institutions of the European Union, the United Nations and governments of other countries.

Digital transformation introduces both new opportunities as well as risks and vulnerabilities that need to be considered and addressed by states, organizations as well as citizens. Digital technologies are used to attack critical infrastructure, interrupt digital services, commit cybercrime, increase surveillance, commit human rights abuses, and spread disinformation. This, in turn, has severe negative impacts for individuals, economy, society and public institutions as well as overall stability in global cyberspace.

The German Federal Foreign Office (FFO) and the European Union (EU) actively promote international cybersecurity policies for a global, open, free, inclusive, stable, and secure cyberspace. Both are committed to work closely with relevant organizations, partners and stakeholders to increase cyber resilience, strengthen cybersecurity capacities and the international cybersecurity architecture. To support this endeavour, the Partnership for Strengthening Cybersecurity has been created in 2023 as one of the German and European instruments to provide technical capacity, foster partnerships and increase public awareness. Its aim is to effectively contribute to the global network of likeminded cooperation partners and to advance cyber capacity building. The program is being implemented by GIZ on behalf of the FFO and co-financed by the European Commission.

The rationale of the project is to contribute to capacities of partner countries to assume increased responsibility for their cybersecurity. Its main goal is the reinforcement of selected bilateral and regional partners' capabilities to prevent, mitigate and respond to cyber security threats and the further development of Germany's cooperation with strategic partners in this area. The regional components of the scalable global project approach initially focus on the Economic Community of West African States (ECOWAS) and African Union (AU), the Western Balkans and Eastern Partnership countries (Armenia, Georgia, Moldova, Ukraine). As gender-specific perspectives are often overlooked in cybersecurity, the FFO is committed to a feminist foreign policy. This approach is implemented through Her CyberTracks, a global training and mentoring program for women in cybersecurity. The project typically works on three areas: 1) Cyber Diplomacy, with policy and diplomatic audiences; 2) Incident Management, with CERT, SOC and technical audiences; and 3) Workforce development, with cyber professionals.

Background Information

The cybersecurity landscape in Armenia is evolving, with the country currently positioned between the initial and mid-levels of cybersecurity maturity. According to the most recent Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU), Armenia ranks 90th out of 181 countries, reflecting significant room for advancement across the five core pillars of cybersecurity: legal, technical, organizational, capacity development, and cooperation.

The overarching policy framework governing cybersecurity in Armenia is the "Information Security and Information Policy Concept", adopted by the President of the Republic of Armenia in 2017. This Concept set out the foundational vision for the country's cybersecurity policy and foresaw the development of a dedicated Cybersecurity Strategy and action plan. However, despite these intentions, no such strategy has been officially adopted to date.

Notable progress was made in 2020 with the approval of a new National Security Strategy by the RA Security Council. This document gave increased priority to cybersecurity and outlined key institutional and legislative actions, including the creation of a national cybersecurity center, establishment of national Computer Emergency Response Teams (CERTs), and the drafting of a Law on Critical Information Infrastructure Protection.

Further institutional development occurred in 2023 with the establishment of the Information Systems Management Board (ISMB), chaired by the Deputy Prime Minister. The ISMB is tasked with ensuring coherence and interoperability across Armenia's digital systems, including cybersecurity aspects. Parallelly, the Information Systems Agency of Armenia (ISAA) was established to consolidate key functions related to cybersecurity and digital governance. While currently operating under the Central Bank of Armenia, ISAA serves as a transitional structure expected to evolve into a permanent National Cybersecurity Center, once the relevant legislation is adopted.

In December 2023, the Ministry of High-Tech Industry released the Draft Law on Cybersecurity, which sets out a comprehensive legal framework for cybersecurity governance in Armenia. The draft law outlines the creation of a centralized National Cybersecurity Agency, tasked with incident response coordination, information sharing, awareness raising, and the protection of critical information infrastructure.

Against this backdrop of institutional reform and legal development, building cybersecurity awareness and capacity across public institutions, both at the state and municipal levels, is a pressing priority. Public servants are increasingly responsible for managing and protecting sensitive data and critical systems. In this context, the development of a structured, accessible, and practical e-learning course on cybersecurity fundamentals is essential. Such a course will enable civil and municipal servants to build strong cyber hygiene practices, better understand and mitigate cyber risks, ensure compliance with evolving legal and regulatory requirements, and actively contribute to Armenia's broader efforts to enhance national cybersecurity resilience.

Learning Objectives:

Upon completion of the course, civil and municipal servants should be able to:

- Understand the basic concepts and principles of cybersecurity and their relevance to public sector operations.
- Apply fundamental cyber hygiene practices to protect personal and institutional digital assets (e.g. secure password management, safe internet use, regular updates).
- Recognize common cyber threats (e.g. phishing, malware, ransomware, social engineering) and understand their impact on individuals and institutions.
- Identify key roles and responsibilities of public servants in safeguarding sensitive data and critical systems.
- Respond appropriately to basic cybersecurity incidents and follow protocols for incident reporting.
- Demonstrate awareness of Armenia's evolving legal and institutional cybersecurity framework, including their obligations under relevant laws and policies.

- Promote a culture of cybersecurity within their institutions by applying safe digital practices and encouraging responsible behaviour among colleagues.

2. Tasks to be performed by the contractor

The contractor is responsible for providing the following services:

Task 1: Review of Available Materials and Stakeholder Consultation
The contractor shall conduct a review of existing cybersecurity training materials focused on fundamental concepts and cyber hygiene practices, including those previously developed by GIZ (e.g. Incident Response Module 1: Fundamentals of Cybersecurity | Review 360) and other relevant partners.

This task includes:

- Identify, collect and review relevant best-practice e-learning and training materials focused on cybersecurity fundamentals.
- Conduct consultations with key stakeholders, including GIZ, the Ministry of High-Tech Industry, ISAA, and other relevant institutions.
- Conduct structured interviews and/or focus group discussions and/or surveys with representatives of the target audience, civil and municipal servants, to understand their practical needs, knowledge gaps, learning preferences, and expectations.
- Identify strengths and limitations of the existing materials and compiling a list of areas that require updates, localization, or further enrichment to ensure the content is relevant and actionable.
- Desing and present a high-level instructional design document (IDD) outlining the course architecture, pedagogical approach, learning objectives, modular structure, delivery approach, and tools to GIZ and relevant stakeholders for feedback and approval.
- The course shall at least cover the following key topics and competency areas: an introduction to the CIA triad (Confidentiality, Integrity, Availability); an overview of various cyber-attacks, including social engineering, phishing, and other prevalent threats; and effective strategies for mitigating cybersecurity risks, such as robust password management, two-factor authentication, data backup protocols, software updates, and the implementation of firewalls and antivirus software. Additionally, the course shall educate public servants on Armenia's cybersecurity-related policies and legislation, relevant government agencies, and standardized operational procedures to follow in the event they suspect they are targets of a cyberattack.
- Propose style guides and templates, comprising of lettering and colours, templates for quizzes and interactions, themes, etc.
- Recommend appropriate authoring tools for the development of the modules for approval by GIZ. If proprietary (commercial) authoring tools are used for the course development, it must be ensured that no license fees or subsequent fees are incurred by GIZ. If media from the authoring tool libraries are used, these must also be license-free. GIZ will not assume responsibility for licensing or copyright-related expenses.

Task 2. Development of the e-learning course

Based on the findings and recommendations from Task 1, the contractor shall design and develop an e-learning course **in Armenian** on cybersecurity fundamentals and cyber hygiene for civil and municipal servants in Armenia. The course should be user-friendly, interactive, and aligned with international best practices in digital learning for adult learners.

- Finalize course objectives, structure, sequencing, and learning outcomes based on the approved instructional design and in consultation with GIZ and stakeholders.

- Consider adaptation and customization of existing materials developed by GIZ to align with the identified training needs and target audience. Incorporate Armenia-specific cyberincident examples into the learning modules.
- Design instructional content using evidence-based learning principles (e.g. problem-based learning, scenario-based activities) to ensure relevance and engagement.
- Develop storyboards or prototypes for each module, including key messages, visuals, interactivity components, and quizzes.
- The structure and duration of each module should be designed to maximize engagement and ensure effective knowledge transfer. Each module should be concise, clearly focused on a specific topic, and structured to maintain a motivating and accessible learning experience. The total seat time for the course should be approximately 1.5 hours, divided into multiple modules. The course should be divided into clearly structured learning modules ("nuggets"), each focused on a single topic or competency area. Each module should not exceed 30 minutes and may be further broken down into short sub-chapters to enhance learner engagement and retention. The overall duration and pacing should be validated through consultation with GIZ and relevant stakeholders.
- Develop the draft course, including voice-over, multimedia, interactive quizzes to enhance learning effectiveness and engagement. All content should follow the design standards and visual identity guidelines agreed with GIZ.
- In terms of multimedia, the contractor ensures consultation and use of adequate design and interactive elements for the modules. The e-learnings should take a multimedia approach to keep the learning experience interesting and engaging. It can include a mix of slides, animations, text, etc. The modules should have at least a mid-level of interactivity, such as enhanced page-turners featuring animated illustrations, clickable elements, synchronized presentation layers. The development of interactive graphics and learning avatars is required. AI-assisted media creation is welcomed, provided that the quality and licensing standards are met.
- All media and graphic elements used in the modules (e.g. photos, graphics, videos) must be either created by the contractor or sourced from freely licensed repositories.
- The course should be inclusive of gender dimensions and further cultural sensitivities in the course materials. The course should be gender-responsive in its content and visualizations.

  Built-in feedback and assessment mechanisms should be incorporated into the course to support learning evaluation and knowledge retention. Each module should include self-assessments, end-of-module quizzes, and user feedback prompts. Assessment types may include multiple choice questions (MCQs), hypothetical scenarios, and matching exercises, designed to evaluate learners' comprehension and application of cybersecurity concepts. These assessments should align with the defined learning outcomes and maintain proportional weightage across the curriculum. Each module must include self-assessments and end-of-module quizzes to support learning evaluation and knowledge retention. Assessment types may include MCQs, scenarios, and matching exercises aligned with the learning outcomes. Successful completion should automatically mark the module as "completed." Sub-module progress should also be trackable. All assessment templates and content shall be developed in consultation with GIZ and relevant stakeholders.

  Upon successful completion of all course modules and assessments, a certificate of completion shall be automatically generated. The certification should be based on learners meeting minimum performance thresholds across the assessment components.

- The Contractor shall ensure that the e-learning is standard compliance, e.g. SCORM or API (reference models, e.g. SCORM 1.2 or SCORM 2004/X-API) in up-to date web standards (e.g. html 5) and without additionally required plug-ins (such as the Adobe Flash Player). The modules must be able to be imported into a standard platform or a learning management system (LMS).
- Conduct an internal review and quality assurance of draft modules. Pilot the modules with a representative group of end users; collect feedback and incorporate necessary revisions to finalize the content.
- Submit draft modules to GIZ and relevant stakeholders for review and feedback.
- After completion, final feedback loop and acceptance by the GIZ, upload the modules onto two designated e-learning platforms as a SCORM package by the contractor and hand over to the client as an HTML5 package via file transfer.
- Transfer all course-related materials (including raw/source files, texts multimedia assets, and editable formats, audiovisual material) to GIZ, ensuring that the content is easy to replicate, manage, and update in the future. All intellectual property rights of the developed content shall be transferred to GIZ upon completion.
- No personal data shall be processed during the creation of the e-learning course(s).

Certain milestones, as laid out in the table below, are to be achieved during the contract term:

Milestones/process steps/partial services	**Deadline**
Task 1: Review of Available Materials and Stakeholder Consultation	July 30, 2025
Task 2: Development of the e-course	October 15, 2025

Period of assignment: from July 2025 until October 2025.

3. Concept

In the tender, the tenderer is required to show *how* the objectives defined in Chapter 2 (Tasks to be performed) are to be achieved, if applicable under consideration of further method-related requirements (technical-methodological concept). In addition, the tenderer must describe the project management system for service provision.

Technical-methodological concept

Strategy (1.1): The tenderer is required to consider the tasks to be performed with reference to the objectives of the services put out to tender (see Chapter 1 Context) (1.1.1). Following this, the tenderer presents and justifies the explicit strategy with which it intends to provide the services for which it is responsible (see Chapter 2 Tasks to be performed) (1.1.2).

The tenderer is required to describe the key **processes** for the services for which it is responsible and create an **operational plan** or schedule (1.4.1) that describes how the services according to Chapter 2 (Tasks to be performed by the contractor) are to be provided.

4. Personnel concept

Team leader

Tasks of the team leader

- Overall responsibility for the advisory packages of the contractor (quality and deadlines)
- Coordinating and ensuring communication with GIZ, partners and others involved in the project.
- Personnel management, in particular identifying the need for short-term assignments within the available budget, as well as planning and steering assignments and supporting short-term experts.
- Oversight of the implementation.
- Regular reporting in accordance with deadlines.

Qualifications of the team leader

- Education/training (2.1.1): university qualification (German ‘Diplom’/Master) in technical/scientific studies (e.g. computer science, business informatics, engineering, natural sciences), social sciences, management or comparable education/qualifications acquired through practical experience (e.g. certifications).
- General professional experience (2.1.3): 10 years of professional experience in project management.
- Specific professional experience (2.1.4): 5 years of professional experience in designing and/or delivering capacity development programmes.
- Leadership/management experience (2.1.5): 5 years of management/leadership experience as project team leader or manager.
- Development cooperation (DC) experience (2.1.7): 3 years of experience in working in/cooperating with DC projects/

Short-term expert pool with 3 members

For the technical assessment, an average of the qualifications of all specified members of the expert pool is calculated. Please send a CV for each pool member (see below Chapter 7 Requirements on the format of the bid) for the assessment.

Tasks of the short-term expert pool

- Fulfil the tasks listed in Chapter 2, including 1) Review of Available Materials and Stakeholder Consultation, 2) Development of the e-course.

Qualifications of the short-term expert pool

- Education/training (2.6.1): university qualification (German ‘Diplom’/Master) in technical/scientific studies (e.g. computer science, business informatics, engineering, natural sciences), social sciences, management or comparable education/qualifications acquired through practical experience (e.g. certifications).

- General professional experience (2.6.3): one expert with 5 years of experience in designing and developing digital learning content or capacity development programmes, one expert with 5 years of experience in production of e-learning materials, one expert with 5 years of experience in multimedia development.

- Specific professional experience (2.6.4): one completed project in e-learning course development for public sector.

The tenderer must provide a clear overview of all proposed short-term experts and their individual qualifications.

5. Costing requirements

Assignment of personnel and travel expenses

Specification of inputs

Fee days	**Number of experts**	**Number of days per expert**	**Total**	**Comments**
Team Leader	1	10	10	
Short-term expert pool	3	20	60	
Transport	**Quantity**	**Number**	**Total**	**Comments**
Travel expenses		1000	1000 km	The number of kilometres is fixed for all tenderers. The travel costs are reimbursed by 120 AMD per km upon provision of evidence. The travel expenses should not be included in the financial offer to be submitted by the Consultant.

6. Inputs of GIZ or other actors

GIZ and/or other actors are expected to make the following available:

- Information on assignments and project context
- Task delivery takes place within the framework of trainings, events or workshops organized by GIZ and/or partners

7. Requirements on the format of the tender

The structure of the tender must correspond to the structure of the ToRs. In particular, the detailed structure of the concept (Chapter 3) should be organised in accordance with the positively weighted criteria in the assessment grid (not with zero). The tender must be legible (font size 11 or larger) and clearly formulated. It must be drawn up in English.

The complete tender must not exceed 10 pages (excluding CVs). If one of the maximum page lengths is exceeded, the content appearing after the cut-off point will not be included in the assessment. External content (e.g. links to websites) will also not be considered.

The CVs of the personnel proposed in accordance with Chapter 4 of the ToRs must be submitted using the format specified in the terms and conditions for application. The CVs shall not exceed 4 pages each. They must clearly show the position and job the proposed person held in the reference project and for how long. The CVs can also be submitted in English.

Please calculate your financial tender based exactly on the parameters specified in Chapter 5 Quantitative requirements. The contractor is not contractually entitled to use up the days, trips, workshops or budgets in full. The number of days, trips and workshops and the budgets will be contractually agreed as maximum limits. The specifications for pricing are defined in the price schedule.