Terms of reference (ToRs) for the procurement of services above the EU threshold

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

CONFIDENTIAL

Project title:	**Processing number/cost centre:**
InnoPA II	**G-012112-001 / G-012216-020**
Country:	**Internal order:**
Egypt	12112010003
Subject of the tender procedure:	**Tender number:**
National Information Sharing and analysis Framework	10017688

0. List of abbreviations 3

1. Context 5

2. Tasks to be performed by the contractor 6

2.1 Term 6
2.2 Objectives, indicators, work packages, milestones 6
2.3 Project and knowledge management requirements 11
2.4 Data protection and information security 13
2.5 Other requirements 13

3. Technical-methodological concept 14

3.1 Interpretation of objectives (section 1.1 of the assessment grid) 14

3.2 Processes and actors in the partner system (section 1.2 of the assessment grid) 15

3.3 Strategy (section 1.3 of the assessment grid) 15

3.4 Project management (section 1.4 of the assessment grid) 17
3.5 Further requirements (section 1.5 of the assessment grid) 18

4. Personnel 18

Expert 1: Team leader (section 2.1 of the assessment grid) 18

5. Costing requirements 24

5.1 Assignment of experts 25
5.2 National administrative staff 25
5.3 Travel expenses 26
5.4 Materials and equipment 27
5.5 Operating costs in the country of assignment 27
5.6 Workshops, education and training 27
5.7 Local contributions 27
5.8 Other costs 27
5.9 Flexible remuneration item 27

6. Requirements on the format of the tender 28

7. Options or follow-on contract 29

7.1 Option to expand the service content/extend the contract term pursuant to section 132 (2) no. 1 German Act against Restraints of Competition (GWB) 29

0. List of abbreviations

- **API:** Application Programming Interface
- **APT:** Advanced Persistent Threat
- **BMF:** Bundesministerium der Finanzen (German Federal Ministry of Finance)
- **CMMI:** Capability Maturity Model Integration
- **CNI:** Critical National Infrastructure
- **CO2:** Carbon Dioxide
- **CSF:** Cybersecurity Framework (NIST)
- **CSO:** Civil Society Organization
- **CV:** Curriculum Vitae
- **DESA:** Department of Economic and Social Affairs (United Nations)
- **DPI:** Digital Public Infrastructure
- **EDR:** Endpoint Detection and Response
- **ENISA:** European Union Agency for Cybersecurity
- **EU:** European Union
- **FIRST:** Forum of Incident Response and Security Teams
- **GIZ:** Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
- **GFFO:** German Federal Foreign Office
- **GRC:** Governance, Risk, and Compliance
- **GTC:** General Terms and Conditions of Contract
- **GWB:** Gesetz gegen Wettbewerbsbeschränkungen (German Act against Restraints of Competition)
- **ICCPR:** International Covenant on Civil and Political Rights
- **ICT:** Information and Communication Technology
- **IEC:** International Electrotechnical Commission
- **ISAC:** Information Sharing and Analysis Center
- **ISAF:** National Information Sharing and Analysis Framework
- **ISO:** International Organization for Standardization
- **ITU:** International Telecommunication Union
- **KOMP:** Kosten-pro-Output-Monitoring und -Prognose (Cost per output monitoring and forecast)
- **LoI:** Letter of Intent
- **MCIT:** Ministry of Communications and Information Technology (Egypt)
- **MOU:** Memorandum of Understanding
- **NDR:** Network Detection and Response
- **NIST:** National Institute of Standards and Technology
- **NTRA:** National Telecom Regulatory Authority (Egypt)
- **PDPC:** Personal Data Protection Centre (Egypt)
- **PDPL:** Personal Data Protection Law (Egypt, Law No. 151 of 2020)
- **PII:** Personally Identifiable Information
- **PN:** Projektnummer / Processing Number
- **RMO:** Risk Management Office
- **SIEM:** Security Information and Event Management
- **SOAR:** Security Orchestration, Automation, and Response
- **SOC:** Security Operations Center
- **SOP:** Standard Operating Procedure

- **STIX:** Structured Threat Information Expression
- **TAXII:** Trusted Automated Exchange of Intelligence Information
- **TIP:** Threat Intelligence Platform
- **TLP:** Traffic Light Protocol
- **ToR:** Terms of Reference
- **ToT:** Train-the-Trainer
- **UDHR:** Universal Declaration of Human Rights
- **UN:** United Nations
- **VgV:** Vergabeverordnung (German Ordinance on the Award of Public Contracts)
- **WBS:** Work Breakdown Structure

1. Context

The present ToR combine services for two different projects working on the intersection of eGovernment and cybersecurity.

Firstly, "**Supporting eGovernment and Innovation in Public Administration (InnoPA)**" is a joint project implemented by the German Agency for International Cooperation (GIZ) in Egypt, on behalf of the German Federal Government, and in partnership with the Ministry of Communications and Information Technology (MCIT). The project aims to strengthen the capacities of the public sector and civil society to drive an inclusive and responsive digital transformation in line with European standards.

The InnoPA project implements a variety of interventions in the areas of institutional capacity building, innovation promotion, digital inclusion, and policy support. The project adopts the principle of "leave no one behind" to ensure that all segments of society benefit from the digital transformation process and enjoy an effective and responsive public administration.

The project has three pillars: 1) Supporting an inclusive, citizen-centred digital transformation of the public sector, the project aims to bridge the digital divide and increase the uptake of existing digital public services. To this end, collaborations with civil society organizations will be carried out to enhance the digital skills of both citizens and civil servants, alongside additional measures focused on strengthening institutional capacity. 2) Promotes innovative solutions for the inclusive and citizen-oriented digital transformation of the public sector. A key part of this effort is the GovTech Innovation Programme, which accelerates startups and the creation of inclusive technological products that enhance government services and responsiveness to citizens' needs and 3) provides support for the development of forward-looking digital strategies and legal frameworks in emerging areas such as trust services, artificial intelligence, and data-driven decision-making, in line with EU digitalization standards.

Within the German Federal Government, the German Federal Foreign Office (GFFO) actively promotes international cybersecurity policies for a global, open, free, inclusive, stable, and secure cyberspace. It is committed to work closely with relevant organizations, partners and stakeholders to increase cyber resilience, strengthen cybersecurity capacities and the international cybersecurity architecture.

In 2023 the German Federal Foreign Office (GFFO) commissioned the second project relevant for these ToR, the "**Partnership for Strengthening Cybersecurity**" which provides technical capacity, fosters partnerships and increases public awareness for a resilient cyberspace. Its aim is to effectively contribute to the global network of likeminded cooperation partners and to advance cyber capacity building. The programme is being implemented by GIZ on behalf of the German Federal Foreign Office, co-financed by the European Commission. The regional components focus on the Economic Community of West African States (ECOWAS), the Western Balkans, and select Eastern Partnership countries (Armenia, Georgia, Moldova, Ukraine), the African Union and the Southern Neighbourhood. The latter is part of the EU-German co-funded Action "Digital Transformation in the Southern Neighbourhood" commissioned by DG MENA, the GFFO and the German Ministry for Economic Cooperation and Development (BMZ) and implemented by GIZ. Outcome 2 focuses on improving prevention preparedness and response of relevant stakeholders in the Southern Neighbourhood regarding cyber threats. In this framework the action supports the improvement of operational capacities, such as prevention, preparedness and response, for

cyber incident management and inter-agency cooperation. In the Egyptian context, the Action cooperates with InnoPA to achieve its project objectives.

In partnership with the National Telecom Regulatory Authority (NTRA) the aim is to build the business framework of the Cybersecurity Information Sharing and Analysis Framework in line with the DPI Safeguard framework.

Both projects – in their respective fields - implement a variety of interventions in the areas of institutional capacity building, innovation promotion, digital inclusion, and policy support. The assignment goal is strengthening Egypt's national cybersecurity resilience by building the framework for Information Sharing and Analysis, enabling secured multi-sector information and the capabilities needed.

The aim of this assignment is to enable NTRA to build the organizational, operational and regulatory requirements and delineating compliance standards for critical infrastructure protection. Moreover, the projects will deliver expertise for cybersecurity and information sharing practises, aligned with recognized international standards (e.g., NIST CSF, ISO/IEC 27001).

2. Tasks to be performed by the contractor

2.1 Term

The expected term of the contract for services must be specified in the 'Special terms and conditions of contract'. The definitive term and service delivery period are set out in the contract award notification.

The planned term for the service provision is 2 years (24 months) from the date of contract signature. All core technical consulting, regulatory framework guidelines, pilot activities, and capacity-building programmes must be successfully delivered and validated within this 24-month operational lifecycle.

2.2 Objectives, indicators, work packages, milestones

The contractor is responsible for achieving the objectives and indicators described in this document.

InnoPA "Supporting e-government and Innovation of Public Administration"

Module objective.

Module objective indicator(s)

The capacity of the public sector and civil society to bring about an inclusive and responsive digital transformation has been strengthened in line with European digitalisation standards

Output 3: Five public institutions that have demonstrated that measures to apply standards for responsible digital governance have been embedded in their workflows.

Output indicator:

3.1 Five improved governance processes for a responsible digital transformation are available to state institutions.

Digital transformation in the Southern Neighbourhood

Outcome

Prevention, preparedness and response of relevant stakeholders in the Southern Neighbourhood with regards to cyber threats is improved

Output 2.2

Improved operational capacities, such as prevention, preparedness and response, for cyber incident management and inter-agency cooperation

Output indicators:

2.2.1 Number of incident response organisations and/or national CERTs created and/or further developed in the target countries

2.2.2 Extent to which the inter-agency cooperation has increased (scale 1-10)

The contractor is responsible for contributing to the previously mentioned Outputs by providing the following work packages and for achieving the corresponding milestones:

1. **Work package 1**: **(Part of Output 3.1 InnoPA) National Information Sharing and Analysis Framework (ISAF)**
    - Legal and policy framework recommendations
    - Define the sectoral ISAC and coordination processes with the most common scenarios.
    - Run a pilot test and provide the report by executing a multi-sector pilot test involving the NTRA and selected Critical National Infrastructure pilot operators to validate the end-to-end ISAF mechanisms in a simulated operational environment in coordination with the NTRA. Then deliver a comprehensive Pilot Evaluation Report detailing: Technical interoperability and API integration

outcomes, evaluation of communication bottlenecks, latency, and procedural friction in coordination channels and identify gaps, compliance findings, and actionable recommendations to optimize the ISAF operating model before full-scale national rollout.

- Formulate Human Rights & Data Protection Safeguards: Deliver concrete policy recommendations aligning NTRA's framework with the Egyptian Personal Data Protection Law (PDPL - Law No. 151/2020), the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) and the African Charter on Human and Peoples' Rights.
- Transparency & Accountability Mechanisms: Design a public reporting model for aggregated, anonymized cyber-incident data and an independent audit framework to periodically evaluate NTRA's information-sharing activities.
- Civil Society Engagement: Define and institutionalize formal communication and co-design channels to ensure civil society organizations (CSOs), academic groups, and public advocates actively participate in the governance and review of the ISAF.
- Critical Asset Interdependencies & Data Taxonomy: Design robust impact assessment methodologies, classification hierarchies (using FIRST-TLP), and pilot test sharing scenarios.
- ISAF Knowledge Transfer Workshops: Conduct targeted knowledge transfer sessions and workshops on the National Information Sharing and Analysis Framework (ISAF), ensuring seamless operational understanding of the legal, regulatory, and policy deliverables among NTRA, MCIT, and sectoral stakeholders

Milestones for work package 1 / Output 3.1	**Delivery period**
ISAF Governance Model (with civil society representation)	To be completed 4 months after contract award
Design of a Secure ISAF Platform and Core Components (Privacy-by-Design verified)	To be completed 8 months after contract award
Develop of Compliance monitoring processes	To be completed 10 months after contract award
Critical asset interdependencies and dependency and analysis methodology	To be completed 12 months after contract award

Data Taxonomy and classification for information exchange	To be completed 14 months after contract award
Legal, Policy, and Human Rights Safeguards Recommendation Paper	To be completed 16 months after contract award
Implementation of sharing protocols (FIRST-TLP / STIX-TAXII)	To be completed 18 months after contract award
ISAF Framework Knowledge Transfer Workshops	To be completed 20 months after contract award
Establishment of sectoral ISACs and coordination processes	To be completed 22 months after contract award
Cross-Sectoral and Safeguard Pilot Tests (documented)	To be completed 23 months after contract award

2. **Work package 2*:* (part of Output 3.1 InnoPA) National Threat Intelligence-Driven Advisory and Design**
    - Define Egypt's Information Sharing and Analysis Framework Architecture.
    - Define the outlines of Egypt's TIP reference architecture (service catalogue, polices & processes/SOPs, functions, capabilities, role matrices).
    - Incorporate Privacy-by-Design in platform requirements: Design strict technical data filters to enforce data minimization (stripping out personally identifiable information (PII) at ingestion) and purpose limitation (guaranteeing that threat feeds are utilized strictly for cybersecurity defence and cannot be repurposed for unauthorized surveillance) as well as other legal requirements according to the Egyptian Personal Data Protection Law (PDPL - Law No. 151/2020).
    - Develop the ISAF Governance and operating model.
    - Architecture of a secure information sharing platform; the core component and functional and non-functional requirements.
    - The technical specification and interfaces within the ecosystem (data model, APIs, mappings, STIX/TAXII profiles).
    - Implement machine-readable artifacts SIEM, EDR, NDR, SOAR tools.
    - Develop templates, forms and checklist used with the defined processes within the scope such as incident, problem, change
    - SOC-CMMI Capability Model and Assessment framework.
    - Design the outline/structure for reports such as incident, compliance, testing etc.
    - Develop critical asset interdependencies and dependencies analysis methodologies and definitions.

Milestones for work package 2 / *Output 3.1*	**Delivery period**
Development of governance and operating model	To be completed 3 months after contract award
Develop TIP Reference Architecture	To be completed 6 months after contract award
Develop of Threat Intelligence Strategy and processes	To be completed 6 months after contract award
Technical specification (Data integration, feeds)	To be completed 12 months after contract award
Incident Management Playbook (policies and procedures)	To be completed 14 months after contract award
Fine tuning of the detection procedures	To be completed 18 months after contract award

Work package 3: (Part of Output 2.2 for the EU Action Digital Transformation in the Southern Neighbourhood):

SANS Specialized Certifications and Capacity Building for NTRA Staff to improve capacities for operationalising the ISAF by strengthening cyber incident management and fostering inter-agency cooperation. To further develop the technical capacities of the national CERT in line with the objectives of the regional EU Action, the service provider should perform the following tasks:

- **SANS Specialized Certification Programme:** Provide/Procure 6 industry-recognized SANS Institute certification training courses along with associated certification exams to selected technical team members from EG-CERT at the NTRA—with specific courses defined according to the targeted priorities and technical needs of NTRA—advancing specialized expertise for cyber incident management. Ensure variety in selected courses in terms expertise and participants from NTRA

- **Knowledge Dissemination Cascade Model:** Structure and supervise a peer-to-peer training model wherein certified NTRA technical members act as internal trainers to cascade knowledge and skills gained from the SANS certifications to colleagues within their respective functional areas.

Milestones for work package 3 / Output 3	Delivery period
Candidate Selection and SANS Certification Plan Finalization (tailored to NTRA priorities and needs)	To be completed 6 months after contract award
Delivery of SANS Certification Trainings & Examinations (6 SANS Certifications)	To be completed 16 months after contract award
Execution of Internal Train-the-Trainer (ToT) Cascade Sessions	To be completed 24 months after contract award

2.3 Project and knowledge management requirements

Requirements on the assignment of experts:

- The contractor is responsible for selecting, preparing and steering the experts assigned to carry out the advisory services.

Requirements on materials and equipment and operating costs:

- The contractor makes the required materials, equipment and consumables available and covers their operating and administrative costs.

Requirements on expenditure management and cost control:

- The contractor manages costs and expenditures, accounting processes and invoicing in line with GIZ requirements.

Monitoring and reporting requirements:

- The contractor plays an active role in the results-based monitoring of the project. Regular monitoring activities must cover at least the following areas
  - Degree to which activities are implemented
  - Degree to which the objectives, indicators and milestones listed in section 2.2 of these ToRs have been achieved
  - Results that have occurred in the contractor's sphere of responsibility
  - Results that have occurred outside the contractor's direct sphere of responsibility

The contractor reports to GIZ as follows:

Instead of the reporting language stipulated in GIZ's General Terms and Conditions of Contract (German), the contractor provides the following reports in the following language: English

- Inception report, *due 3 months after contract signature the contractor must deliver the first document which includes the TIP reference architecture and the defined operating and governance model*
- Interim report(s)
  - Progress reports every 6 months
  - Final Report on the project completion status 2 weeks before the end of the contract
  - The interim report(s) and the final report should provide information about the progress made towards objectives in each of the monitoring areas specified above.

Requirements for company-wide learning, knowledge and innovation:

- The contractor provides support in implementing a project evaluation with special emphasis on ensuring the effectiveness of the knowledge management process.

- The contractor expresses willingness, if required, to support project assistants or staff members on temporary placements who, in the context of GIZ's separately financed training programmes for junior employees, work in and undertake special tasks for the project.
- All outputs related to work package 1 and 2 must adhere to GIZ InnoPA's branding and communication guidelines and all outputs related to work package 3 must adhere to the EU Action "Digital Transformation in the Southern Neighbourhood" communication guidelines, which will both be provided to the contractor by the project team upon contract signature.

Backstopping requirements:

The contractor ensures appropriate backstopping. The following services form part of the standard backstopping package. In accordance with GIZ's General Terms and Conditions for supplying services and work on behalf of the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, these services – as well as the ancillary personnel costs – must be priced into the fee schedules of the staff listed in the tender:

- The contractor's responsibility for its own staff;
- Ensuring the flow of information between GIZ and the contractor's field staff;
- Process-oriented technical and conceptual steering of the consulting services;
- Steering adaptations to changing framework conditions;
- Performance monitoring;
- Ensuring the administrative management of the project;
- Ensuring compliance with reporting requirements;
- Technical support by the contractor's staff for its personnel on the ground;
- Making local use of and sharing the lessons learned by the contractor with the GIZ team.

2.4 Data protection and information security

The provisions on data protection and information security of the current version of GIZ's General Terms and Conditions of Contract (sections 1.7. Confidentiality and 1.11 Data protection) apply.

In addition, the contractor must explicitly ensure that all activities and deliverables under this contract must be aligned with the Egyptian Personal Data Protection Law (PDPL - Law No. 151/2020), the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the African Charter on Human and Peoples' Rights, and the African Convention on Cybersecurity and Personal Data Protection. And that the proposed national framework implements the following **minimum technical and legal thresholds**:

1. **Privacy by Design & Data Minimization:** The framework and secure platform must strictly collect and process only the structural technical telemetry data (e.g., indicator IP addresses, file hashes, malware signatures) necessary for identifying and mitigating cyber threats.
    - Technical pipelines must include automated sanitization phases to strip out extraneous PII, sensitive personal data, and communication content before any automated information exchange occurs.
2. **Purpose Limitation:** Information shared within the ISAF and across sectoral ISACs must be utilized **solely** for cybersecurity defence, threat mitigation, and infrastructure resilience.
    - Legal agreements, and SOPs governing the platform must explicitly prohibit the repurposing of this data for non-security monitoring, mass surveillance, commercial reuse, or arbitrary personal profiling.
3. **Oversight & Judicial Control:**
    - The policy recommendations must state that any exceptional access or caveats based on "national security" must be strictly defined by law, necessary, and proportionate in a democratic society.
    - Any requests to deviate from the standard personal data protection thresholds for national security purposes must be subject to **independent judicial control and prior judicial authorization**.
4. **Transparency & Public Accountability:**
    - The framework must support public, aggregated, and completely anonymized reporting on cyber threat trends and systemic vulnerabilities to raise overall public security awareness without exposing individual data.

All cybersecurity and data-sharing operations under NTRA's purview must be designed to accommodate periodic independent external audits evaluating technical integrity, compliance with the Egyptian PDPL, and respect for fundamental human rights.

2.5 Other requirements

Safeguards and gender measures with specific reference to services:

In order to promote gender equality and avoid or mitigate possible unintended negative impacts in its area of responsibility, the contractor should implement the following measures:

- Gender equality:

Gender-Sensitive Communication & Material Design: Design all instructional resources, framework documentation, policies, and training materials using gender-inclusive terminology and layout standards.

- Environmental protection and climate action (climate change mitigation/adaptation):
  Green Computing Principles: Formulate technical platform recommendations (Work Package 1) that prioritize energy-efficient software design, carbon-optimized cloud hosting pathways, and minimized server telemetry processing loads.
- Conflict and context sensitivity:
  Non-Stigmatization Guidelines: Require that all threat analysis taxonomies and attribution models remain strictly technical and objective, prohibiting any platform features that associate specific domestic societal groups, demographics, or geographical regions with threat indicators.
- Human rights:
  Mitigation of unintended digital surveillance: Actively integrate sanitization scripts to prevent the framework from being used to collect, index, or parse user traffic logs or communications, thereby safeguarding the citizens' fundamental right to privacy.

The contractor's staffing profile should be balanced in terms of gender and age.

3. Technical-methodological concept

In this section, the tenderer is required to reflect on the objectives and terms of reference of the tender at hand, describe the partner system and its processes in the area of responsibility and present the technical-methodological concept for completing the tasks listed in section 2 and achieving the set objectives. In addition, the tenderer must describe the design of the project management process.

3.1 Interpretation of objectives (section 1.1 of the assessment grid)

The tenderer is required to interpret the objectives for which it is responsible. Simple repetition of the objectives formulated in section 2 of the ToRs is not desired. Rather, the contractor is to describe and interpret the changes in the partner system that are to be directly achieved by the object of the tender procedure. The resulting positive impact on the partner system (section 1.1.1 of the assessment grid) should also be presented.

The contractor must undertake a critical examination of the ToRs (section 1.1.2 of the assessment grid), by:

- undertaking an assessment of the appropriateness of the personnel concept for implementing the scheduled tasks;
- providing an assessment of the results hypotheses for achieving the objectives and possible risks in implementation;
- making an assessment of the technical concept

3.2 Processes and actors in the partner system (section 1.2 of the assessment grid)

Processes describe actions or sets of tasks that are necessary in order to render specific services in a sector or in the cooperation/partner system. Specific actors are given responsibility for determining and implementing these actions and sets of tasks in line with the regulations. Actors are usually institutions such as ministries, local governments, associations and chambers, non-governmental organisations, companies in a sector or individual businesses, universities or banks, but may also be individuals (e.g. a person with higher decision-making authority).

The tenderer is required to describe, using existing documents where possible (see annexes), the processes in the sector or partner system that are relevant to the services put out to tender (section 1.2.1 of the assessment grid).

The tenderer is required to present the actors (partners and others) who are relevant for the tender in the form of a map of actors. As far as possible, it should list the actors by name. Their mandates as well as strengths, weaknesses and interests with respect to the services put out to tender are also to be briefly presented (section 1.2.2 of the assessment grid).

In addition, the tenderer is required to describe the interaction between the actors mentioned above. This can consist of a description of the specific collaboration between individual actors in the processes listed above, of the dependencies or conflicts between the actors and their consequences or of existing dialogue and communication formats (section 1.2.3 of the assessment grid).

3.3 Strategy (section 1.3 of the assessment grid)

The strategy for delivering the services in the tender is the core element of the technical-methodological concept. It is composed of the following elements:

- Procedure for achieving the objectives stated in section 2.2 of these ToRs
- Development of partnerships with the relevant actors
- Approaches for leverage effects and measures for scaling-up
- Consideration of environmental and social compatibility requirements (including gender equality)
- Appropriate consideration of further requirements

3.3.1 Strategic approach to achieving the objectives mentioned in the ToRs (section 1.3.1 of the assessment grid)

The tenderer is required to describe and justify the approach it plans to adopt in order to achieve the milestones, objectives and results (see section 2) for which it is responsible.

The tenderer is expected to explain both:

1. *Strategic Approach to Tasks (Section 2):* A conceptual strategy addressing the cybersecurity, trust-building, and regulatory objectives (focusing on strategic logic and *why* specific methodologies are chosen, rather than a mere description of activities).

2. *Implementation Strategy:* Concrete, operational lines of action and key milestone activities demonstrating *how* the prescribed ToR strategy and requirements will be systematically deployed and executed over the 2-year term.

3.3.2 Building partnerships with the relevant actors
(section 1.3.2 of the assessment grid)

The tenderer is required to develop and describe a strategy for developing the cooperation with the actors in the partner system who are relevant for the implementation of the services in the tender. The project partnerships already mentioned in section 1 must also be taken into account.

3.3.3 Approaches for leverage effects and measures for scaling-up
(section 1.3.3 of the assessment grid)

The tenderer is required to state whether there are promising approaches for leverage effects beyond the measures mentioned in section 2 (for example through targeted measures in the field of 'knowledge management') and to describe them. In doing so, the tenderer is required to present and explain measures that promote both horizontal and vertical scaling-up. In particular, the tenderer must submit proposals on how innovations that have been developed in the context of implementation can be disseminated beyond the sphere of influence of the project.

3.3.4 Consideration of environmental and social compatibility requirements
(section 1.3.4 of the assessment grid)

Gender equality

The tenderer is required to outline in the tender how it can prevent negative impacts on gender equality in its area of responsibility and how it can contribute to improving gender equality through corresponding measures (see also relevant requirements in section 2.5).

Environmental protection and climate action (climate change mitigation/adaptation)

The tenderer is required to outline in the tender how it can prevent negative impacts on the environment and the climate in its area of responsibility and, in addition, how it can contribute to improving the environmental and climate situation through corresponding measures (see also relevant requirements in section 2.5).

Conflict and context sensitivity

The tenderer is required to outline in the tender how it is planning its activities in the context of conflicts or violence and what specific measures it has adopted for conflict- and context-sensitive implementation (see also relevant requirements in section 2.5).

Human rights

The tenderer is required to outline in the tender how it can prevent negative impacts on the human rights situation in its area of responsibility and how it can contribute to improving the human rights situation through corresponding measures (see also relevant requirements in section 2.5).

Requirement: 'Gender equality':	2 points out of 10 (maximum)
Requirement: 'Environmental protection and climate action (climate change mitigation/adaptation)':	2 points out of 10 (maximum)
Requirement: 'Conflict and context sensitivity':	2 points out of 10 (maximum)
Requirement: 'Human rights:	4 points out of 10 (maximum)

3.4 Project management
(section 1.4 of the assessment grid)

In this section, the tenderer presents the operational plan for implementing the services in the tender, describes the procedure for coordination with GIZ or the project and the project partners, and explains its monitoring procedure.

3.4.1 Operational plan
(section 1.4.1 of the assessment grid)

The tenderer is required to draw up and explain an operational plan for implementing the strategy described in section 3.3, including a plan for the assignment of all the experts included in the tender. The operational plan must include the assignment times (periods and expert days) and assignment locations of the individual experts, the milestones as presented in section 2 and, in particular, describe all the necessary work stages in detail and in chronological order. The tenderer can define further milestones beyond those prescribed in section 2 and map them out in the plan of operations.

3.4.2 Coordination with GIZ or the commissioning project
(section 1.4.2 of the assessment grid)

In the tender, the tenderer is required to describe the procedure for coordinating with GIZ or with the commissioning project.

3.4.3 Steering or coordination of measures with the relevant implementing partner
(section 1.4.3 of the assessment grid)

In the tender, the tenderer is required to name the implementing partners relevant for implementing the services and to describe and explain the procedure for steering or coordinating the measures with them.

3.4.4 Monitoring

(section 1.4.4 of the assessment grid)

In the tender, the tenderer is required to describe how it can ensure that the requirements resulting from the monitoring system of the project or the partner are met (see section 2). In doing so, the tenderer is required to describe how the information that is relevant for monitoring is collected and in what form and at what intervals monitoring data are updated.

3.5 Further requirements

(section 1.5 of the assessment grid)

- The tenderer is required to explain how they will navigate the national context and provide explanations of how it will make use of national resources (for example national institutions, network partners etc.) in the context of service delivery.
- The tenderer is required to describe its backstopping strategy. A CV must be provided for the positions for technical and administrative backstopping.

4. Personnel

The tenderer is required to provide 'experts' for the positions referred to and described (scope of tasks and qualifications) in this section on the basis of corresponding CVs. **The requirements on the format and content of the CVs are described in section 6.**

The qualifications mentioned below correspond to the requirements for achieving the highest number of points in the technical assessment.

'One year of professional experience' is therefore defined as a cumulative 12 expert months with at least 18 expert days per month, provided no diverging definition is specified for individual qualifications.

Expert 1: Team leader (section 2.1 of the assessment grid)

This position is a key expert.

Tasks of expert 1:

- Manage and coordinate all contractor activities and outputs under work package 1, work package 2 and work package 3.
- Ensuring the coherence and complementarity of the contractor's services with other services delivered by the project at local and national level
- Design, implementation, monitoring and evaluation of capacity development measures for local partners in cyber security covering key areas of governance (NIST CSF, ISO 27001, SOC-CMM maturity), architecture (TIP reference designs, STIX/TAXII sharing protocols), operations (incident playbooks, response drills), and regulatory compliance (personal data protection, data minimization, privacy-by-design controls).

- Responsibility for taking cross-cutting themes into consideration (for example, gender equality) in project activities
- Staff management, in particular identifying the need for short-term assignments within the available budget, planning and managing the assignments and supporting experts
- Ensuring that monitoring procedures are carried out
- Regular reporting in accordance with deadlines
- Responsibility for checking the use of funds and financial planning in consultation with the commission manager at GIZ
- Supporting the commission manager in updating and/or adapting the project strategy, in evaluations and in preparing a follow-on phase

Qualifications of expert 1 (Team Leader):

Education/training (section 2.1.1 of the assessment grid):	Master's degree in Computer Engineering, Computer Science, Cybersecurity, Information Security Management, or Systems Engineering.
Language (section 2.1.2 of the assessment grid):	Knowledge of English, C1 - level in the Common European Framework of Reference for Languages
General professional experience (section 2.1.3 of the assessment grid):	15 years of professional experience in the ICT sector.
Specific professional experience (section 2.1.4 of the assessment grid):	10 years of professional experience in national-level cybersecurity governance, 3 years in working on strategy development, and 3 years' experience in working on international standards (ISO/IEC 27001, NIST CSF).
Leadership/management experience (section 2.1.5 of the assessment grid):	10 years of management experience in IT projects, companies or other organisations with disciplinary leadership responsibility for 10 people and an annual budget responsibility for EUR 500 000.
International professional experience outside the country/region of assignment (section 2.1.6 of the assessment grid):	5 years of professional experience in the EU
Professional experience in the country/ region of assignment (2.1.7 of the assessment grid):	1 year of professional experience working on cyber security in the North Africa region (in accordance with UN DESA Statistics Division)
Experience in the field of development cooperation (section 2.1.8 of the assessment grid):	5 years of experience in development cooperation projects

Expert 2: Senior Threat Intelligence Architect (section 2.2 of the assessment grid)

This position is a key expert.

Tasks of expert 2

- Designing comprehensive, multi-sector national threat intelligence blueprints incorporating automated security indicator exchange protocols.
- Defining national Security Operations Center (SOC) operational hierarchies, service catalogues, and standardized incident escalation workflows.
- Establishing a secure Threat Intelligence Platform (TIP) reference architecture to manage centralized ingestion, normalization, and correlation of telemetry data.
- Translating complex threat detection parameters into machine-readable rules and active playbooks for SIEM, EDR, NDR, and SOAR tools.
- Leading technical design blocks, multi-stakeholder security workshops, and integration pilots to validate secure indicator sharing.

- Qualifications of expert 2.

Education/training (section 2.2.1 of the assessment grid):	Master's degree in Computer Engineering, Computer Science, Information Security, Network Security, or Software Engineering.
Language (section 2.2.2 of the assessment grid):	Knowledge of English, C1 level in the Common European Framework of Reference for Languages
General professional experience (section 2.2.3 of the assessment grid):	9years of professional experience in the sector of ICT
Specific professional experience (section 2.2.4 of the assessment grid*):*	6 years of experience in designing Threat Intelligence Platforms (TIP) (5/10 points) and 3 years of experience designing Monitoring Center architectures (SIEM/SOAR/EDR) using MITRE ATT&CK. (5/10 points)
Leadership/management experience (section 2.2.5 of the assessment grid):	5 years of management experience in IT projects or teams with disciplinary leadership responsibility for 5 people.
International professional experience outside the country/region of assignment (section 2.2.6 of the assessment grid):	5 years of professional experience in the EU.
Professional experience in the country/ region of assignment (2.2.7 of the assessment grid):	1 year of experience working on cyber security in the North Africa region. (in accordance with UN DESA Statistics Division)
Experience in the field of development cooperation (section 2.2.8 of the assessment grid):	3 years of experience in development cooperation projects.

Expert 3: Regulatory, Data Protection & Information Sharing Specialist (section 2.3 of the assessment grid)

This position is a key expert.

Tasks of expert 3

- Leading the multi-sectoral governance design, sectoral ISAC coordination models, and information-sharing legal/policy frameworks.
- Directly overseeing the integration of human rights, data protection (PDPL Law 151/2020), and privacy-by-design principles to mitigate unintended surveillance or abuse risks.
- Proposing independent judicial control models over national security caveats.
- Planning public transparency initiatives and civil society engagement processes.

Qualifications of expert 3.

Education/training (section 2.3.1 of the assessment grid):	Master's degree in Law (LL.M. in Information Technology Law, Data Protection Law, or Human Rights Law) or Master's degree in Cybersecurity Policy.
Language (section 2.3.2 of the assessment grid):	Knowledge of English, C1 level in the Common European Framework of Reference for Languages
General professional experience (section 2.3.3 of the assessment grid):	9 years of professional experience in ICT Regulatory Affairs.
Specific professional experience (section 2.3.4 of the assessment grid*):*	8 years of experience in designing governance frameworks, with incorporating data protection, privacy-by-design safeguards, and human rights compliance (UDHR, ICCPR, African Charter) within digital infrastructure frameworks.
Leadership/management experience (section 2.3.5 of the assessment grid):	5 years of management in multi-stakeholder organizations.
International professional experience outside the country/region of assignment (section 2.3.6 of the assessment grid):	5 years of professional experience in the EU.
Professional experience in the country/ region of assignment (2.3.7 of the assessment grid):	1 year of experience working on the Cyber security topic in the North Africa region. (in accordance with UN DESA Statistics Division)
Experience in the field of development cooperation (section 2.3.8 of the assessment grid):	3 years of experience in development cooperation projects.

Expert 4: Governmental Liaison & Ecosystem Advisor (section 2.4 of the assessment grid)

This position is a key expert

Tasks of expert 4

- Providing strategic advice on the Egyptian cybersecurity landscape, specifically regarding national administrative procedures and the regulatory environment.
- Acting as the primary facilitator for communication and coordination between the service provider and Egyptian government entities, including the NTRA, relevant ministries, and critical national infrastructure operators.
- Researching and providing the international team with all necessary local data, including national laws, regulatory updates, and sector-specific governmental requirements.
- Supporting the design and delivery of internal capacity-building initiatives and "Train-the-Trainer" programmes within the public administration.

Qualifications of expert 4.

Education/training (section 2.4.1 of the assessment grid):	Master's degree in digital transformation in public administration, digital public policy or digital law.
Language (section 2.4.2 of the assessment grid):	Knowledge of Arabic, C2 level in the Common European Framework of Reference for Languages (5/10 points) Knowledge of English, C1 level in the Common European Framework of Reference for Languages (5/10 points)
General professional experience (section 2.4.3 of the assessment grid):	9 years of professional experience in the Egyptian ICT governmental sector.
Specific professional experience (section 2.4.4 of the assessment grid*):*	9 years of professional experience in the Egyptian cybersecurity ecosystem, with 4 years' experience working with the NTRA operations, national security protocols, and local administrative structures.
International professional experience outside the country/region of assignment (section 2.4.6 of the assessment grid):	3 years of professional experience working on cyber security with international organizations, European companies, or donor-funded projects.
Professional experience in the country/ region of assignment (2.4.7 of the assessment grid):	9 years of professional experience in Egypt, with 4 years' experience of navigating local government ICT entities and regulatory bodies.
Experience in the field of development cooperation (section 2.4.8 of the assessment grid):	3 years of experience in development cooperation projects.

Expert 5: Pool of Experts 2-5 experts (section 2.5 of the assessment grid)

To judge the ability of the tenderer to offer the pool of experts required here, **2 CVs** – keeping in mind the requested profiles – need to be added. The ability is assessed solely on the basis of these exemplary CVs.

The actual number of experts assigned from the pool may differ from the number of experts required in section 4 of the Terms of Reference. For experts not named in the tender, GIZ must confirm before the assignment that their qualifications are equivalent to those of the short-term experts proposed in the tender.

Tasks of the expert pool

- Support the developing ISAF
- Support to develop the incident Management playbook
- Support in developing the technical architecture artifacts.
- Run the pilot tests and document the reports.
- Participate in the technical workshops

Qualifications of the expert pool

Education/training (section 2.5.1 of the assessment grid):	Bachelor's degree in Computer Engineering, Computer Science, Cybersecurity, or Information Technology.
Language (section 2.5.2 of the assessment grid):	2 experts with knowledge of English, C1 level in the Common European Framework of Reference for Languages. (5/10 points) 1 expert with knowledge of Arabic, C2 level in the Common European Framework of Reference for Languages. (5/10 points)
General professional experience (section 2.5.3 of the assessment grid):	2 experts with 6 years of professional experience in the ICT sector
Specific professional experience (section 2.5.4 of the assessment grid):	2 experts with 3 *years* of *professional* experience in Cybersecurity and SOC operations
Leadership/management experience (section 2.5.5 of the assessment grid):	2 experts with 3 years of experience in technical cyber security projects (5/10 points) 1 expert with 2 years of experience in specialized training modules. (5/10 points)
International professional experience outside the country/region of assignment (section 2.5.6 of the assessment grid):	1 expert with 1 year of experience working on the Cyber security topic in the North Africa region. (in accordance with UN DESA Statistics Division)

Professional experience in the country/ region of assignment (2.5.7 of the assessment grid):	1 expert with 2 years of professional experience in Egypt

UN DESA regions are defined as East Africa, Central Africa, North Africa, Southern Africa, West Africa, South America, the Caribbean, Central America, North America, Central Asia, East Asia, South Asia, Southeast Asia, West Asia/Middle East, Eastern Europe, Northern Europe, Southern Europe, Western Europe, Australia, Melanesia, Micronesia and Polynesia; refer to USND methodology for country assignment.

The tenderer must assign all the proposed experts to the required qualifications and clearly present them in a separate table preceding the CVs. The summary presentation must mention only qualifications that are actually indicated in the CVs. Professional experience must be evidenced by meaningful references in the CVs. It is advisable to make explicit reference to each example of professional experience.

Soft skills of team members

In addition to their specialist qualifications, all team members are also expected to have the following qualifications:

- Team skills
- Initiative
- Communication skills
- Sociocultural and intercultural skills
- Efficient partner- and client-oriented working methods
- Interdisciplinary thinking

Soft skills are not evaluated.

5. Costing requirements

In your tender, please do not deviate from the specification of inputs required in these ToRs (the number of experts and expert days, the budget specified in the price schedule). This is part of the competitive tender and is used to ensure that the tenders can be compared objectively. Please note: only services that were commissioned by GIZ and rendered by the contractor will be remunerated. We would also like to point out that it may not be necessary to make use of the total number of proposed expert days.

5.1 Assignment of experts

The number of expert days corresponds to full working days.

Expert	Expert days in the country of residence /remote	Availability of expert in the country of assignment* in expert days	Expert days in total	Consecutive stay > 3 months (see General Terms and Conditions, section 3.6.2)	Number of international flights	Number of national flights
Expert 1:						
Team Leader	30	10	40	No	2	0
Expert 2:				No		0
Senior Threat Intelligence Architect	50		50		0	
Expert 3:						0
Regulatory, ISAF & Information Sharing Specialist	50		50	No	0	
Expert 4:						
Local Expert (Governmental Liaison & Ecosystem Advisor)	0	50	50	No	0	0
Expert 5:						
Pool of Experts	80		80	No		

5.2 National administrative staff

– Not applicable –

5.3 Travel expenses

5.3.1 Travel – sustainability considerations

GIZ would like to reduce greenhouse gas emissions (CO_2 emissions) caused by travel. When preparing your tender, please incorporate options for reducing emissions, for example by selecting the lowest-emission booking class (economy) or using means of transport, airlines and flight routes that are more CO_2-efficient. For short distances, travel by train (second class) or e-mobility are the preferred options.

CO_2 emissions caused by air travel must be offset. GIZ specifies a budget for this, through which the carbon offsets can be settled against evidence.

There are many different providers in the market for emissions certificates, and they have different climate impact ambitions. The Development and Climate Alliance has published a list of standards (only in German available). GIZ recommends using the standards specified there.

5.3.2 Travel expense requirements

The travel expenses must be costed as follows by the contractor:

Travel expenses item	Quantity/budget
Total number of international flights	2
Total number of regional/national flights	0
CO2 offsets for flights	140 EUR
Link to working aid and table for setting the budget	An unalterable budget for CO2 offsets for settlement against evidence is specified.
Transport costs (rail travel, car travel, public transport)	10
Per-diem allowances	10
Accommodation allowances	10
Other travel expenses (visa, project-related travel expenses outside the place of business etc.)	NA

Per-diem allowances are reimbursed as a lump sum up to the maximum amounts permissible under tax law for each country as set out in the country table in the circular from the German Federal Ministry of Finance on travel expense remuneration (download at https://www.bundesfinanzministerium.de).

In addition, for the following items, reasonable costs can be settled against evidence up to the proposed amount.

- Flight costs
- Transport costs
- Other travel expenses

Notes on the settlement of accommodation allowances outside Germany

For the country Egypt, tenderers may offer accommodation allowances up to EUR 168. This is the maximum amount permissible under tax law as per the BMF circular on travel expense reimbursement.

5.4 Materials and equipment

– Not applicable –

5.5 Operating costs in the country of assignment

– Not applicable –

5.6 Workshops, education and training

– Not applicable –

5.7 Local contributions

– Not applicable –

5.8 Other costs

Budget for Delivery of 6 SANS Certifications: EUR 48,000.00

The fixed, unalterable budget above is earmarked in the price schedule for the delivery of SANS Certification Trainings & Examinations (6 SANS Certifications)

5.9 Flexible remuneration item

Budget for flexible remuneration: EUR 28,000.00

The fixed, unalterable budget above is earmarked in the price schedule for flexible remuneration. Flexible remuneration is intended to facilitate the flexible management of the contract by the commission manager at GIZ. The contractor can make use of the funds in accordance with section 3.6.5.7 of the General Terms and Conditions.

6. Requirements on the format of the tender

The structure of the tender must correspond with the structure of the ToRs. It must be legible (for example Arial, font size 11 or larger) and clearly formulated. The technical tender must be written in English.

The technical-methodological concept of the tender (section 3 of the ToRs) must not exceed 10 pages (not including the cover page, list of abbreviations, table of contents, brief introduction and CV for the backstopper). Additional annexes not requested will not be assessed. External content (e.g. links to websites) will also be disregarded.

The CVs of the staff proposed in accordance with section 4 of the ToRs must be in the EU format and not more than four pages in length. The CVs can also be submitted in English.

The CVs must clearly and unequivocally show what position the proposed person held, which tasks they performed and how long they worked during which period in the specified references. **The references contained in the CVs must therefore include the following information:**

- Name of the company/organisation/reference project in which the expert worked
- Position held and task(s) performed by the expert in the company/organisation/reference project
- Work outcomes or products produced by the expert, or expert's contribution to the completion of these outcomes and projects (if relevant)
- Duration of the expert's assignment in the company/organisation/reference project per calendar year in full-time expert days, weeks or months (for example: 2019: 2 months, 2020: 10 months, 2021: 1 month)
- Leadership experience/management: clear information on the reference projects or fixed positions within the company/organisation in which the requirements specified in section 4 were fulfilled (for example, period, number of persons for whom the expert had disciplinary responsibility, project budget)
- International professional experience/professional experience in the country of assignment: clear information on the reference projects or fixed positions in the company/organisation in which the requirements specified in section 4 were fulfilled (for example, actual duration of assignment on the ground in full-time expert days, weeks or months)

In order to facilitate the assessment, we request that you number the references sequentially and provide only references that are clearly related to the object of this tender.

7. Options or follow-on contract

7.1 Option to expand the service content/extend the contract term pursuant to section 132 (2) no. 1 German Act against Restraints of Competition (GWB)

GIZ can exercise the following option if it wishes to expand the tendered services. This is described in detail below.

Nature and scope:

While retaining the overall character of the contract, there is a possibility of GIZ continuing to obtain the services specified in section 2 of these Terms of Reference and/or of expanding the contract to include further services of the same kind. The items shown in section 5 (Costing requirements) of these Terms of Reference can be increased by up to EUR 62,900.00. Within this framework, the options can be exercised in up to two parts.

The option number of expert days corresponds to full working days.

***