

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

Cybersecurity Awareness Campaign and Trainings	Project number/ cost centre: G-018082-001
---	--

0. List of abbreviations	2
1. Background	3
2. Tasks to be performed by the contractor	5
Delivery Approach	15
Milestones and Deadline for the Consultancy	17
3. Concept.....	17
Technical-methodological concept	17
Project management of the contractor (1.6)	18
4. Personnel concept.....	18
Team leader/ Cybersecurity and Capacity-Building Expert	18
Key expert 1: Communications and Media Expert	19
5. Costing requirements	20
Assignment of personnel and travel expenses	20
Sustainability aspects for travel	20
6. Requirements on the format of the tender	22

0. List of abbreviations

BMZ	Federal Ministry for Economic Cooperation and Development
CSA	Cyber Security Authority
DPC	Data Protection Commission
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
GEA	Ghana Enterprises Agency
PSInno	Private Sector and Innovation Promotion in Ghana
RBM	Results-Based Monitoring
SMEs	Small and medium-sized enterprises
ToRs	Terms of reference

1. Background

The Private Sector and Innovation Promotion in Ghana (PSInno) project is part of the German Federal Ministry for Economic Cooperation and Development (BMZ) core theme, "Training and Sustainable Growth for Good Jobs in Ghana". The project is being implemented by Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH in collaboration with Ministry of Trade, Agribusiness and Industry. The objective of the project is to strengthen the competitive and employment-promotion economic development in selected sectors in Ghana, particularly in the north of the country.

PSInno supports growth-oriented small and medium-sized enterprises (SMEs) in Ghana with a focus on agribusiness, digital economy and innovation. Building on earlier private sector and entrepreneurship initiatives. In the agricultural and food sector, the programme targets producers, SMEs, and innovative enterprises in northern Ghana, whilst in the digital economy it targets all companies including startups and freelancers. PSInno works as a facilitator alongside business development service providers and financial institutions to improve market access, strengthen skills, and promote innovative business models. At the macro level, PSInno works with national and regional stakeholders to develop or reform policy instruments, contributing to an improved business environment for SMEs, while working with intermediaries to introduce new or adapted institutionalised support services to strengthen the competitiveness of companies in selected sectors.

The programme pursues an integrated approach to agricultural value chain development and digital economy promotion, providing technical advisory support to public and private partners, strengthening intermediary organisations, and building the capacities of companies, startups, and smallholder farmers to enable sustainable business growth.

1.1 Context

Ghana's digital economy is growing rapidly, creating new opportunities for SMEs across sectors. The adoption of digital tools and platforms, e-commerce channels, and mobile money services is increasingly essential to SME competitiveness, market access, and sustainable growth. However, increased digitalization also exposes businesses to a growing range of cyber threats, data breaches, online fraud, and mobile money scams- risks that many SMEs are poorly equipped to manage.

The Cyber Security Authority (CSA) is mandated to ensure cybersecurity regulation, coordination, and awareness in Ghana, while the Data Protection Commission (DPC) is the statutory body responsible for data protection regulation and the registration of data controllers and data processors in Ghana.

For growth-oriented SMEs, cybersecurity and data protection compliance are not merely technical or regulatory obligations; they are increasingly important business enablers. Compliance with cybersecurity standards and data protection regulations can support access to formal markets, attract investment and clients, facilitate participation in digital supply chains, and meet the expectations of domestic and international trading partners. Conversely, SMEs that are unable to demonstrate basic cybersecurity and data protection compliance may face barriers to accessing growth opportunities and markets.

Several factors constrain SME market access and growth while undermining cybersecurity resilience and competitiveness in Ghana: low awareness and poor cyber hygiene, mobile money fraud, limited awareness of cybersecurity and data protection compliance pathways, and low levels of digital trust. These challenges are further compounded by the limited capacity of intermediary institutions, including innovation hubs, the Ghana Enterprises Agency (GEA),

and sector associations, on which SMEs rely for business support. Many of these institutions do not yet offer cybersecurity or data protection advisory services as part of their existing SME services. For this phase, the Volta Region is proposed as the pilot region due to its proximity to Accra, CSA's existing presence and access to SME data, and its vibrant SME ecosystem and established business associations. These factors will facilitate efficient coordination, stakeholder engagement, baseline assessment, and monitoring, while generating lessons to inform subsequent implementation and scale-up in Northern Ghana and potentially other regions.

In response to these challenges, CSA, in collaboration with DPC, has requested support from the GIZ-implemented PSInno to position cybersecurity and data protection compliance as strategic drivers of SME competitiveness, scalability, and market readiness under the DigiShield Ghana initiative.

DigiShield Ghana

DigiShield Ghana is a collaborative initiative of CSA, DPC, and the GIZ-implemented PSInno. The project is designed to strengthen cybersecurity resilience, data protection compliance, and digital trust among growth-oriented SMEs in Ghana, thereby improving their competitiveness, market access, and capacity for sustainable and scalable growth.

The initiative recognizes that cybersecurity and data protection compliance are particularly important for businesses that transact digitally, handle customer data, or seek to participate in formal supply chains. These businesses have both significant risk exposure and considerable potential to benefit from improved compliance and market credibility.

The primary target groups of the initiative are growth-oriented SMEs, including startups operating in the digital economy, as well as business intermediaries and multiplier organizations. These intermediaries include innovation hubs, GEA, and sector associations that can integrate cybersecurity and data protection advisory support into their existing SME services, thereby extending the reach of the initiative beyond direct beneficiaries. Across these target groups, priority will be given to women-led and youth-led enterprises.

The initiative's training, advisory, and awareness activities are organised around four thematic areas: cybersecurity fundamentals, data protection compliance, mobile money fraud prevention, and digital safety for business operations. These themes reflect the most pressing risks and compliance gaps identified for SMEs in Ghana and provide a consistent structure across training content, advisory materials, campaign messaging, and monitoring of SME practice adoption throughout the assignment.

1.2. Objective of the Consultancy

To strengthen the cybersecurity and data protection resilience of growth-oriented SMEs in the Volta Region and build the institutional capacity of intermediaries to deliver institutionalised cybersecurity and data protection advisory support services to SMEs in selected sectors.

The specific objectives of this assignment are to:

- I) Establish a comprehensive evidence base on the cybersecurity and data protection needs, awareness levels, behavioural triggers and compliance gaps of participating SMEs and intermediaries in the Volta Region and map the relevant stakeholder landscape to inform targeted and context-specific programme engagement.
- II) Support CSA and partners to co-develop a practical, contextually relevant, and institutionally validated training package covering cybersecurity fundamentals, data

protection and DPC compliance, mobile money fraud prevention, and digital safety, tailored to the distinct needs and roles of SMEs and intermediary organisations.

- III) Together with CSA and partners, co-design and deploy a coordinated DigiShield Ghana awareness and media campaign across the Volta Region that shifts how SMEs, intermediaries, and business support actors understand and communicate about cybersecurity and data protection — from regulatory obligation to business growth enabler and from understanding to behavioural change.
- IV) Deliver practical cybersecurity and digital safety training to growth-oriented SMEs in the Volta Region and verify the adoption of safer digital practices among participants through structured post-training follow-up and behavioural assessment.
- V) Build and institutionalise cybersecurity and data protection advisory capacity in selected intermediary organisations, equipping 15 intermediary staff with the training, tools, and referral pathways needed to independently support SMEs beyond the life of the intervention.
- VI) Consolidate implementation results, document lessons learned and produce actionable recommendations to inform the scale-up of DigiShield Ghana to Northern Ghana and beyond.

2. Tasks to be performed by the contractor

The consultant is expected to perform the following tasks along with associated deliverables in collaboration with CSA:

Task 1: Needs Assessment and Stakeholder Mapping of Intermediaries and SMEs in the Volta Region

Objective: Establish an evidence base on the cybersecurity and data protection awareness levels, practices, behavioural trigger or blockages and compliance gaps of participating intermediaries and SMEs in the Volta Region and map the relevant stakeholder landscape to inform targeted and context-specific programme engagement.

Specific Tasks & Deliverables

S/N	Task	Deliverables
1.1	Review the existing needs assessment conducted by CSA to establish baseline findings on SMEs' cybersecurity knowledge, practices, and risk exposure in the Volta Region.	SME Cybersecurity and Data Protection Needs Assessment Report highlighting key compliance gaps, readiness levels, behavioural and organisational barriers, priority support needs, and profiles of SMEs and intermediaries to inform targeted training and advisory interventions.
	Complement this review with direct engagement with a sample of SMEs to assess their current cybersecurity and data protection practices, awareness of CSA and DPC requirements, data handling arrangements, compliance readiness and organisational capacity. The assessment should identify the key factors that prevent SMEs from adopting compliant practices, including knowledge,	

resource, capacity and behavioural barriers, and determine what support and interventions are required to enable sustained behavioural change.

- | | | |
|-----|--|--|
| 1.2 | Identify, map, and analyse enterprise support organisations (ESOs) and business intermediaries operating in the Volta Region, including business associations, innovation hubs, financial service providers, and relevant government agencies. Assess and prioritise identified stakeholders based on their services, reach, institutional relationships, and capacity to support programme delivery and sustainability. Assess the intermediary organisations to document current cybersecurity practices, familiarity with CSA and DPC regulatory requirements, existing data handling arrangements, and organisational readiness to adopt baseline compliance measures. Document existing funding and business models (e.g. membership fees, donor/grant funding, fee-for-service arrangements) of ESOs to inform the viability of monetized or comparable-value sustainability options under Task 6. | Stakeholder Mapping Matrix presenting a structured landscape of relevant intermediaries in the Volta Region, with a prioritised engagement plan and targeted outreach recommendations. |
| 1.3 | Develop clear, documented selection criteria for participating SMEs and intermediaries. Apply the criteria to assess and select organisations for training, prioritising SMEs in the agribusiness and digital economy sectors and applying women-led and youth-led enterprise participation as a cross-cutting selection principle. | Documented selection criteria and a finalised list of selected SMEs and intermediaries, with a brief justification of selection decisions against the established criteria. |

Expected Outcome: A well-grounded, evidence-based understanding of the cybersecurity and data protection landscape and behavioural triggers among SMEs and intermediaries in the Volta Region, providing the programme with a clear and actionable starting point for targeted engagement.

Task 2: Development of Training Materials and Institutionalized Services for Intermediaries and SMEs

Objective: Develop a practical, contextually relevant training package on cybersecurity, data protection, mobile money fraud, and digital safety, tailored to the capacity levels, sectoral contexts, and compliance obligations of participating intermediaries and SMEs in the Volta Region that can be turned into a service by ESOs.

Building directly on the findings of Task 1, the consultant will design and develop a structured training package that translates cybersecurity and data protection requirements into accessible and actionable learning for business audiences. Additionally, the consultants will work with the CSA, DPC and SMEs to design institutionalized support services that ESOs can monetize and use to support SMEs. The training materials will be tailored to the distinct roles and needs of

intermediaries and SMEs. Intermediaries will be equipped to provide ongoing advisory support to SMEs beyond the intervention, while SME training will focus on practical compliance and behavioural change in their day-to-day operations.

Specific Tasks & Deliverables

S/N	Task	Deliverable
2.1	Develop training content on cybersecurity fundamentals and baseline controls for intermediaries and SMEs, grounded in CSA requirements under the Cybersecurity Act. Content will cover access management, data handling procedures, device and network security, and incident reporting protocols, with intermediary-facing materials designed to support ongoing advisory delivery to SMEs beyond the intervention.	Facilitator-ready session guide and participant workbook on cybersecurity fundamentals, including practical exercises and case studies drawn from Ghanaian business contexts, differentiated for intermediary and SME audiences.
2.2	Develop training content on data protection and DPC compliance, covering the Data Protection Act, DPC registration procedures, consent management, data subject request handling, and breach notification obligations. Intermediary materials will include guidance on supporting SMEs through the DPC registration process as part of their advisory role.	Facilitator-ready session guide and participant workbook on data protection and DPC compliance, including a step-by-step DPC registration guide and practical compliance checklists for SME use, differentiated for intermediary and SME audiences.
2.3	Develop training content on mobile money fraud prevention, covering common fraud typologies including SIM swap scams, social engineering, and fake payment requests, as well as practical verification and incident response protocols relevant to SME business operations.	Facilitator-ready session guide and participant workbook on mobile money fraud prevention, including scenario-based exercises and a practical fraud response protocol template adapted for SME contexts.
2.4	Develop training content on digital safety for business operations, covering the safe use of digital platforms, e-commerce tools, and business communication channels, with a focus on building sustainable digital hygiene habits among SME owners and staff.	Facilitator-ready session guide and participant workbook on digital safety, including a digital hygiene self-assessment tool and practical guidance on securing commonly used business platforms and communication tools.
2.5	Drawing on the intermediary funding and business model data gathered under Task 1.2, map and develop viable services or models that ESOs can institutionalize either as a paid offering or as added value within their existing operations, informed by comparable examples from similar advisory services elsewhere. This mapping should directly inform the design of the toolkit and facilitator guide, so the advisory service is built around a defined service concept from the outset.	Service model mapping brief, informing toolkit design and to be finalised per-intermediary later under Task 6 (following implementation experience).
2.6	Co-facilitate a structured 4-day co-creation workshop with representatives from CSA, DPC, and GIZ to review, develop and validate draft training materials under Tasks 2.1 to 2.4, and to co-develop the communication and	Workshop report documenting proceedings, decisions, and agreed revisions; finalised and institutionally validated training

	branding materials outlined in Task 3. The workshop will ensure that all materials reflect the institutional perspectives, regulatory accuracy, and branding requirements of all three partner organisations before deployment.	package incorporating inputs from CSA, DPC, and GIZ; and a co-developed set of communication and branding materials ready for deployment under Task 3.
--	---	--

Task 2 Note:

- All materials will be developed in plain, jargon-free language appropriate for business audiences without a technical background, and adapted for delivery in the Volta Region context, including consideration of local language accessibility where relevant.
- Materials will be designed for reuse and adaptation by intermediaries, supporting sustainability beyond the life of the intervention.

Expected Outcome: A complete, contextually grounded, validated and immediately deployable training package that directly addresses the cybersecurity, data protection, mobile money fraud, and digital safety gaps identified in Task 1.

Task 3: Development of Communication, Branding, and Media Materials

Objective: Develop approved communication, branding, and media materials to support a targeted awareness campaign that builds on behavioural science findings and positions cybersecurity and data protection compliance as a business growth enabler for SMEs in the Volta Region and beyond.

The consultant will develop a cohesive suite of communication, branding, and media materials under the DigiShield Ghana identity. The materials will be designed to reach SMEs, business intermediaries, financial institutions, business associations, and the broader public, communicating key messages on cybersecurity, data protection, and mobile money fraud prevention in a manner that is accessible, compelling, and actionable for non-technical business audiences.

Specific Tasks & Deliverables

S/N	Task	Deliverable
3.1	Develop the DigiShield Ghana campaign identity and branding framework, establishing consistent visual and messaging standards to be applied across all communication and media materials produced under this task.	DigiShield Ghana brand and messaging guide, including logo usage, colour palette, tone of voice, and core campaign messages for each thematic area.
3.2	Develop print and digital information materials for SME, intermediaries and public audiences, covering cybersecurity fundamentals, data protection compliance, mobile money fraud prevention, and digital safety for business operations.	A set of co-branded materials covering four (4) thematic areas: 1 fact sheet, 1 infographic, and 1 one-page guidance notes, designed for both print distribution and digital sharing across social

		media and business platforms, available in English and adapted for local language accessibility where relevant.
3.3	Develop audio-visual and broadcast materials for community radio and digital media channels, translating key campaign messages into formats suitable for broadcast in the Volta Region, yet scalable for use at other parts of the country.	One set of radio scripts and recorded audio spots covering the four campaign thematic areas, and at least one short-form video asset suitable for social media and digital platforms, co-branded by CSA, DPC, and GIZ.
3.4	Develop event and presentation materials to support the awareness campaign rollout, stakeholder engagement activities, and the Cybersecurity Month dialogue session under Task 4.	One (1) co-branded event materials including one (1) presentation deck, two (2) pull-up banners, and one (1) campaign one-pager suitable for distribution at business events, trade fairs, and stakeholder meetings.
3.5	Obtain formal review and approval of all materials from CSA, DPC, and GIZ prior to deployment, incorporating institutional feedback and ensuring regulatory accuracy across all content.	Approval documentation confirming sign-off from CSA, DPC, and GIZ on the full suite of communication and media materials.

Task 3 Notes:

- The materials will carry the combined institutional weight of CSA, DPC, and GIZ, lending credibility and regulatory authority to the campaign messaging across all channels and audiences.
- SMEs, intermediaries, business associations, and the broader public in the Volta Region will have access to clear, accessible, and contextually relevant information on cybersecurity risks, data protection obligations, and mobile money fraud prevention — delivered through formats and channels suited to their operating environment, including print, digital, and community radio.
- Beyond the immediate campaign, the expected outcome is a reusable communications asset that extends the reach and sustainability of DigiShield Ghana beyond the intervention period.
- Intermediaries and partner institutions (CSA, DPC, etc) will be equipped with materials they can deploy independently in their ongoing SME engagement, ensuring that the campaign narrative continues to reach new audiences after the formal programme concludes.

Expected Outcome: A fully developed, institutionally approved, and deployment-ready suite of communication, branding, and media materials that present cybersecurity and data protection compliance as a tangible business advantage for SMEs rather than a regulatory requirement.

Task 4: Implementation of Awareness and Media Engagement Campaigns

Objective: Facilitate the implementation of a coordinated awareness and media engagement campaign, led by CSA and DPC, by coordinating agreed media activities, disseminating

approved materials across targeted channels, and monitoring, documenting, and reporting on campaign coverage and reach.

Building on the materials developed and approved under Task 3, the consultant will support CSA and DPC in executing the DigiShield Ghana awareness campaign across the Volta Region and document lessons learned to scale the initiative.

Specific Tasks & Deliverables

S/N	Task	Deliverable
4.1	Coordinate and facilitate the dissemination of approved DigiShield Ghana communication and branding materials on behalf of CSA and DPC over a 3-to-4-week campaign period. This includes coordination with community radio stations, Community Information Centres, sector association meetings, and digital platforms in the Volta Region, covering all associated logistics and costs.	Campaign plan and implemented media campaign, with documented evidence of materials disseminated, channels activated, organisations and audiences reached, and associated logistics managed.
4.2	Conduct at least 2 targeted community radio engagements in the Volta Region to amplify key DigiShield Ghana messages on cybersecurity awareness, data protection compliance, and mobile money fraud prevention, complementing digital and print outreach channels.	Summary report of radio engagements conducted, including stations, airtime secured, broadcast dates, estimated audience reach, and recorded copies of aired content.
4.3	Coordinate and support CSA and DPC engagement with print and digital media in the Volta Region targeting SME and business audiences at the regional level.	Media engagement report documenting media houses contacted, coverage secured, publication or broadcast dates, and an aggregated estimate of campaign reach across regional media channels.
4.4	Monitor and document all campaign activities, coverage, and reach throughout the implementation period, tracking performance against agreed targets and capturing qualitative evidence of shifts in SME and stakeholder positioning on cybersecurity and data protection compliance in the Volta Region.	Campaign monitoring report presenting reach and coverage data across all channels, qualitative evidence of messaging uptake, lessons learned, and recommendations for sustaining campaign momentum beyond the intervention period.

Task 4 Notes:

- The consultant's role is facilitative while CSA and DPC retain institutional leadership and public visibility throughout. The role will include coordinating logistics, managing dissemination, and ensuring campaign activities are implemented as planned.
- All campaign activities will reinforce the core DigiShield Ghana narrative: that cybersecurity and data protection compliance is a business growth enabler, not a regulatory burden.

Expected outcome: The awareness campaign will have been implemented across the Volta Region, with measurable reach across agreed channels and evidence of a shift in how SMEs

and intermediaries position cybersecurity and data protection compliance, from regulatory obligation to business growth enabler.

Task 5: Delivery of SME Cybersecurity and Digital Safety Training

Objective: Deliver practical, targeted cybersecurity, data protection, momo fraud and digital safety training to growth-oriented SMEs in the Volta Region and verify the adoption of safer digital practices following training completion.

Building on the training materials developed and validated under Task 2, the consultant will deliver one structured 2-day training workshop for a single cohort of 35 selected SME participants in the Volta Region. The same cohort will attend both days, ensuring continuity of learning and progressive engagement across all training modules.

Specific Tasks & Deliverables

S/N	Task	Deliverable
5.1	Co-facilitate delivery of one 2-day practical training workshop for a single cohort of 35 selected growth-oriented SMEs in the Volta Region, on a non-residential basis. The workshop will cover all modules developed under Task 2. Training content and sequencing will be adapted to the specific needs, sectors, and capacity levels of participating SMEs as established during Task 1.	Training completion report documenting workshop proceedings, modules delivered, daily attendance records disaggregated by gender and sector, participant feedback, and a summary of key results against agreed training output indicators.
5.2	Provide structured post-training implementation support to at least 50% of participating SMEs to help them institutionalise cybersecurity and data protection measures and establish simple referral and redress channels to CSA and DPC where needed. Support will verify adoption of agreed behavioural indicators across all training modules — including multi-factor authentication, data backup procedures, DPC registration progress, fraud verification processes, and privacy notices — using a pre and post assessment framework consistent with the RBM Matrix established during inception.	Post-training implementation support report documenting follow-up check-ins completed, action plans issued, adoption of behavioural indicators per module, and institutionalised referral and support channels connecting participating SMEs to CSA and DPC.

Task 5 Notes:

- Training delivery will be informed by the needs assessment and selection process completed under Task 1, ensuring content is contextually relevant and appropriately pitched to the capacity levels and operating realities of participating SMEs.
- All training activities will prioritise the participation of women-led and youth-led enterprises as a cross-cutting commitment throughout delivery.
- Trainings will be delivered primarily by CSA and DPC staff, with the lead will co-facilitate providing technical backstopping and ensuring content delivery remains consistent with the developed training materials and agreed methodology.

Expected Outcomes: By the end of Task 5, 35 growth-oriented SMEs in the Volta Region will have completed practical training across all DigiShield Ghana modules, with at least 50% demonstrating verifiable adoption of safer digital practices and connected to functional referral and support channels with CSA and DPC.

Task 6: Capacity Building and Institutionalisation of Cybersecurity, and Digital Safety Advisory Support for Intermediary Institutions

Objective: Build the capacity of SME intermediary organisations in the Volta Region to provide institutionalised, independent cybersecurity, data protection and digital safety advisory support to SMEs beyond the life of the intervention.

The consultant will deliver a structured 2-day training workshop for intermediary staff. The workshop will build on the training modules and advisory materials developed under Task 2 and consider options for monetizing this advisory service by the intermediary organisations. The workshop will equip them with the knowledge, tools, and referral pathways needed to institutionalise cybersecurity and data protection advisory support within their regular SME services. The consultant will then help the ESOs to institutionalize a service that can be monetized or turned into comparable value for the ESOs.

Specific Tasks & Deliverables

S/N	Task	Deliverable
6.1	Co-facilitate delivery of one 2-day training workshop for a single cohort of 15 intermediary staff including GEA and innovation hubs in the Volta Region, on a non-residential basis. The same cohort will attend both days.	Training completion report documenting modules delivered, daily attendance disaggregated by gender and organisation, participant feedback, and a summary of results against agreed training output indicators.
6.2	Develop and hand over a practical advisory toolkit package to each participating intermediary organisation, enabling independent delivery of basic cybersecurity and data protection advisory support to SMEs after the consultancy concludes.	Finalised advisory toolkit package for each participating intermediary, comprising the practical guidance resource, diagnostic checklist, and facilitator guide, reviewed and approved by CSA and DPC prior to handover.
6.3	Support participating intermediaries to integrate the advisory toolkit and diagnostic checklist into their regular SME service offerings, providing guidance on how cybersecurity and data protection advisory support can be embedded into existing intake processes, business advisory sessions, and SME support programmes.	Integration support report documenting the guidance provided to each intermediary, agreed integration approaches, and any adaptations made to the toolkit or checklist to suit each organisation's service model.
6.4	Establish a defined referral pathway for each participating intermediary, providing clear, documented routes for referring SMEs with cybersecurity or data protection needs beyond	Referral pathway document for each participating intermediary, specifying referral triggers, contact points, and escalation procedures for CSA, DPC, and

	the intermediary's own advisory capacity to CSA, DPC, or other specialist support organisations.	relevant specialist support organisations.
6.5	Conduct a single structured follow-up check-in with all participating intermediaries approximately 4 weeks after toolkit handover, to support early use of the advisory toolkit, address implementation challenges, and confirm that referral pathways are operational.	Intermediary follow-up check-in report documenting the status of toolkit adoption, early implementation issues identified and addressed, and confirmation of referral pathway operationalisation across all participating intermediary organisations.
6.6	Building on the service model mapping developed under Task 2 and the findings from the follow-up check-in (6.5), finalise a sustainability model for at least 50% of participating intermediaries, as a paid offering or added value, tailored to their business model and early implementation experience.	Sustainability and value model brief for at least 50% of participating intermediaries, outlining a recommended approach and practical next steps.

Task 6 Notes:

- Participating intermediaries will leave the intervention as capable, resourced advisory touchpoints for SMEs navigating cybersecurity and data protection compliance.
- The toolkit will include a practical cybersecurity, data protection, and digital safety guidance resource aligned to all Task 2 modules; a diagnostic checklist aligned to the core behavioural indicators used in the needs assessment and SME training pre and post assessment to enable intermediaries to assess SME gaps; and a facilitator guide enabling intermediary staff to make referrals or independently deliver structured advisory sessions with SMEs using the toolkit and checklist.

Expected Outcome: By the end of Task 6, selected intermediary organisations in the Volta Region will be independently equipped to provide ongoing cybersecurity and data protection advisory support to SMEs, with the tools, knowledge, and institutional pathways needed to sustain that support well beyond the life of the intervention.

Task 7: Results Documentation, Learning, and Programme Closeout

Objective: Consolidate implementation results and participant feedback, document lessons learned across all programme activities, update training and advisory materials based on evidence gathered, and produce actionable recommendations to inform the scale-up of DigiShield Ghana.

Specific Tasks & Deliverables

S/N	Task	Deliverable
7.1	Collect structured feedback from participating SMEs and intermediary organisations across all programme activities, covering training quality and relevance, post-training support, campaign engagement, and overall programme experience.	Consolidated feedback and results report documenting participation data disaggregated by gender, sector, and organisation type; implementation progress against agreed output indicators; and a synthesis of feedback from SMEs and intermediaries across all tasks.

7.2	Identify and document key lessons learned from implementation, drawing on consolidated feedback, post-training assessment results, intermediary follow-up check-ins, and campaign monitoring data.	Lessons learned report presenting findings by task and thematic area, with clear implications for programme design, delivery, and partnership arrangements in future implementation cycles.
7.3	Revise and finalise the training materials and the intermediary advisory toolkit based on lessons learned and participant feedback, producing final versions that are polished, validated, and ready for reuse in future training and advisory delivery.	Final, updated training package and intermediary advisory toolkit, incorporating revisions based on implementation evidence and approved by CSA, DPC, and GIZ for future use.
7.4	Develop forward-looking recommendations to inform the scale-up of DigiShield Ghana, with particular focus on Northern Ghana as the next priority geography, drawing on evidence from the Volta Region pilot to inform target group selection, delivery modalities, partnership arrangements, and resource requirements.	Recommendations report presenting a structured, evidence-based case for DigiShield Ghana scale-up, with specific guidance on adapting the programme for the Northern Ghana context.

Notes:

- Feedback will be collected through agreed instruments such as structured surveys or focus group discussions and consolidated alongside participation records, activity logs, and key results documented throughout implementation.
- Lessons will be organised by task and thematic area to provide a structured, actionable account of what worked, what did not, and why.

Expected Outcome: By the end of Task 7, DigiShield Ghana will have a validated evidence base, updated programme materials, and actionable recommendations ready to inform its scale-up in Northern Ghana and beyond.

Overall Expected Outcomes (Tasks 1-7):

DigiShield Ghana will have strengthened the cybersecurity and data protection resilience of growth-oriented SMEs in the Volta Region, improved the capacity of multiplier ESOs or intermediary organisations to provide ongoing advisory support, and advanced a measurable shift in how SMEs and business support actors understand and act on cybersecurity and data protection compliance.

At the institutional level, CSA and DPC will have deepened their engagement with the private sector, with validated tools, trained intermediaries, and established referral pathways that extend their regulatory reach into the SME ecosystem beyond the life of the intervention.

At the programme level, GIZ will have generated a documented, evidence-based pilot in the Volta Region, with updated materials, lessons learned, and actionable recommendations that provide a credible foundation for scaling DigiShield Ghana to Northern Ghana and other priority geographies under the PSInno project.

Delivery Approach

In conducting the relevant tasks specified, the consultant shall undertake the following, among other relevant tasks identified by the consultant or CSA/DPC/GIZ:

I. Inception and Coordination

The contractor shall:

- Engage with the GIZ, CSA, DPC and relevant project partners to confirm the assignment objectives, target groups, training needs, geographic focus, implementation arrangements, and stakeholder roles.
- Develop a detailed implementation plan covering the reviewed needs assessment, training activities, awareness campaign, and media activities, key milestones, and delivery schedule.
- Maintain regular coordination with CSA, DPC, GIZ, and relevant project stakeholders throughout the assignment to ensure alignment, timely decision-making, and effective implementation.
- Ensure that all data protection content developed under the assignment is reviewed and validated by the DPC prior to finalisation.

II. Project Management, Results Communication and Reporting

- **Quality Assurance:** The consultants are responsible for ensuring the quality of all outputs delivered under this contract. Quality assurance measures should include direct collaboration and validation of outputs with CSA, DPC and GIZ, and incorporation of feedback from GIZ within agreed timelines. GIZ reserves the right to request revisions to any output that does not meet the required standard, and the consultant is expected to incorporate feedback promptly and without additional cost.
- **Risk Mitigation and Technical Safeguards:** The consultants should create and maintain a live risk and mitigation register throughout the contract period, to actively manage institutional, operational, and data-handling liabilities throughout the assignment. Because the training deals directly with sensitive digital safety and cybersecurity data, this tracking mechanism will include strict operational protocols to ensure total data privacy during systemic assessments and fieldwork, aligning with national and internal GIZ data protection regulations.
- **Project Communication**
All communication between the consultant and GIZ, CSA, DPC and other relevant stakeholders shall be conducted in accordance with GIZ's communication guidelines and standards. This includes written correspondence, presentation of outputs, use of GIZ branding and templates where required, and engagement with media or the public on matters related to the consultancy. The consultant should ensure that all communication is professional, timely, and appropriately cleared with GIZ before dissemination to external audiences.
- **Project Documentation and Reporting Content**
In support of project management and reporting, the contractor shall produce the following: (1) Professional photos from the activities, especially training workshops in

accordance with GIZ standards (2) Work with the communication team within GIZ to produce content for social media.

- **Inception Report to GIZ:** Due within 2 weeks of contract start date, this report should present the consultant's detailed understanding of the assignment, a refined work plan with updated milestones, a risk assessment, and the proposed monitoring framework with baseline values where applicable.
- **Bi-Weekly Updates with GIZ:** The consulting team is required to hold bi-weekly check-in meeting (virtual/in-person) with the GIZ PSInno project team throughout the contract period. These sessions serve as a regular touchpoint for progress updates, early identification of challenges, coordination on upcoming activities, and alignment on any adjustments to the work plan.
- **Final Report to GIZ:** Due at least two weeks before the end of contract period. The final report should provide a comprehensive account of all main tasks, outputs delivered, an assessment of results achieved against indicators, challenges, lessons learned, potential opportunities and recommendations for sustaining and building on the results of the consultancy beyond the contract period.

III. Monitoring, Evaluation, Learning and Adaptation

The contractor shall establish a structured GIZ Results-Based Monitoring (RBM) Matrix during the inception phase, defining baseline indicators and target metrics for the needs assessment, training, awareness and capacity-building activities, with data collection workflows incorporating gender-disaggregated training participation targets. The RBM Matrix shall include a pre/post assessment to measure changes in intermediaries and SME practices resulting from training and implementation support, tracked against core behavioural indicators – including adoption of multi-factor authentication (MFA), data backup procedures, fraud-verification processes, privacy notices, or other agreed practices – in addition to participation and awareness metrics. The contractor shall track and document implementation progress, including intermediary and SME participation, training delivery, training delivery, behavioural indicator results, awareness and media activities, intermediary engagement and key results against agreed indicators and targets; collect participant feedback following training and capacity-building activities; and document lessons learned, good practices and recommendations arising from implementation to inform future engagements.

Contribution to PSInno Results Framework

The outputs of this consultancy contribute directly to two indicators under the PSInno Results Framework:

- Output 1, Indicator 1.2 – Institutionalised Support Services: The consultancy will support the CSA and selected intermediary organisations in the Volta Region to establish and institutionalise cybersecurity and data protection advisory services as part of their regular SME support offering. This will strengthen the capacity of intermediaries to provide ongoing, structured support to SMEs beyond the immediate intervention.
- Output 3, Indicator 3.2 – Competence Development in Digital Technology: The SME training activities will contribute directly to this indicator by enabling participating SMEs

to develop practical competencies in cybersecurity and data protection, which are recognised qualifying domains under the indicator.

The consultant shall collect, document, and report the relevant results data in a format that enables GIZ to update its project monitoring system. The consultant shall also coordinate closely with the GIZ PSInno team throughout implementation to ensure that results measurement and reporting are aligned with the applicable indicator definitions, measurement methodology, data requirements, and reporting timelines.

Knowledge management and scaling: The contractor shall identify institutional lessons learned, operational challenges, and effective practices arising from implementation, building on the documentation required under Task 8. These insights shall inform practical recommendations for scaling the approach – including implementation in Northern Ghana – under the broader DigiShield Ghana initiative.

Milestones and Deadline for the Consultancy

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

Milestones	Deadline
Inception Report with work plan	14 th December 2026 (2 weeks after contract start date)
Program Implementation	December 2026 – May 2027
Final Reporting to GIZ	15 th July 2027

Period of assignment: from 30th November 2026 to 30th July 2027.

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.

Note: The numbers in parentheses correspond to the lines of the technical assessment grid.

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 **Error! Reference source not found.** 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 present the actors relevant for the services for which it is responsible and describe the **cooperation (1.2)** with them.

The tenderer is required to present and explain its approach to **steering** the measures with the project partners (1.3.1) and its contribution to the **results-based monitoring system** (1.3.2).

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 **Error! Reference source not found.** (Tasks to be performed by the contractor) are to be provided. In particular, the tenderer is required to describe the necessary work steps and, if applicable, take account of the milestones and **contributions** of other actors (partner contributions) in accordance with Chapter 2 (Tasks to be performed) (1.4.2).

The tenderer is required to describe its contribution to knowledge management for the partner (1.5.1) and GIZ and to promote scaling-up effects (1.5.2) under **learning and innovation**.

Project management of the contractor (1.6)

The tenderer is required to explain its approach for coordination with the GIZ project. In particular, the project management requirements specified in Chapter 2 (Tasks to be performed by the contractor) must be explained in detail.

The tenderer is required to draw up a **personnel assignment plan** with explanatory notes that lists all the experts proposed in the tender; the plan includes information on assignment dates (duration and expert days) and locations of the individual members of the team complete with the allocation of work steps as set out in the schedule.

4. Personnel concept

The tenderer is required to provide personnel who are suited to filling the positions described, on the basis of their CVs (see Chapter 6), the range of tasks involved and the required qualifications.

The below specified qualifications represent the requirements to reach the maximum number of points in the technical assessment.

Team leader/ Cybersecurity and Capacity-Building Expert

Tasks of the team leader

- Lead overall implementation, team coordination, and communication with GIZ, CSA, DPC, and partners.
- Review the existing CSA needs assessment, identify gaps, and lead stakeholder mapping in the Volta Region.
- Lead development of training content, tailored to intermediaries and SMEs in agribusiness and digital economy, with attention to women- and youth-led enterprises.
- Coordinate CSA and DPC as training facilitators and provide technical backstopping.
- Lead post-training implementation support, verifying intermediary and SME adoption of agreed behavioural indicators (MFA, backups, fraud-verification, privacy notices).
- Lead intermediary capacity building, including the advisory toolkit (guidance, checklist, referral pathway), with the facilitator guide developed jointly with the Communications Expert
- Document activities, feedback and lessons learned, including behavioural evidence-based recommendations to inform the design and improvement of future initiatives, and prepare the inception and final reports

Qualifications of the team leader

- Education/training (2.1.1): Advanced university degree (Master's or equivalent) in cybersecurity, information technology, computer science, digital technology, information systems, project management, or a related field (8/10). Relevant professional cybersecurity certification(s) would be an advantage (2/10).
- Language (2.1.2): Fluent in English (8/10). Proficiency in Ewe is a significant advantage (2/10).
- General professional experience (2.1.3): 10 years of general professional experience, including 3-5 years' experience in cybersecurity, digital safety, IT/ICT, training and capacity building, or SME/private-sector support. Experience reviewing existing research or assessment data and closing gaps through consultation (e.g., KIIs), is required.
- Specific professional experience (2.1.4): Working knowledge of cybersecurity and data protection for SMEs, private-sector organisations, hubs or intermediaries (4/10). Demonstrated experience applying behavioural science or related approaches to support sustained adoption of new practices, tools, or service models, evidenced by relevant prior assignments (3/10). Direct experience working within Ghana's SME ecosystem and understanding of Ghana's cybersecurity and data protection environment (3/10).
- Leadership/management experience (2.1.5): 5 years of management or team leadership experience, preferably leading multidisciplinary teams; ability to turn assessment findings into practical recommendations and manage timelines across stakeholders.
- Regional experience (2.1.6): 5 years of experience in projects in Ghana. Experience working with SMEs in Volta Region would be an advantage.
- Development cooperation (DC) experience (2.1.7): Prior experience working on GIZ or similar donor-funded projects is a significant advantage.
- Other (2.1.8): Strong written, verbal and facilitation skills required.

Key expert 1: Communications and Media Expert

Tasks of Communications and Media Expert

- Lead development of communication concepts, key messages and branded assets (radio jingles, banners, posters, fact sheets, social media graphics, digital and video content)
- Lead translation and localization of selected materials into the two target Ghanaian languages (Ewe and Twi).
- Lead implementation of the awareness and media engagement campaign, including coordination of radio engagements, media house and journalist liaison, and digital dissemination.
- Monitor and document campaign activities, coverage, and reach.
- Support SME training workshops as needed, including co-facilitating sessions and practical exercises with CSA, DPC and the Team Leader.
- Contribute to the facilitator guide in the intermediary advisory toolkit, with the Team Leader leading technical content
- Contribute to the documentation of campaign results, participant feedback, lessons learned, and recommendations.

Qualifications of Communications and Media Campaign Expert

- Education/training (2.2.1): University degree in Communications, Marketing, Media Studies, Public Relations, or a related field.
- Language (2.2.2): Fluent in English (8/10). Proficiency in Ewe is a significant advantage (2/10).
- General professional experience (2.2.3): 5 years professional experience in communications, media or public awareness campaigns, or marketing, including campaign strategy, content development, and media coordination.
- Specific professional experience (2.2.4): Demonstrated experience developing and implementing multi-channel campaigns (radio, print, digital, social media), including managing translation and localisation. Experience supporting or co-facilitating training or capacity-building sessions is required. Cybersecurity or digital safety experience is an advantage
- Regional experience (2.2.6): Experience working in Ghana and familiarity with the local media landscape.
- Development Cooperation (DC) experience (2.2.7): Experience in DC projects is an advantage; familiarity with donor-funded project environments including GIZ is a significant advantage.
- Other (2.2.8): Strong creative, facilitation, and communication skills; good analytical and reporting skills.

5. Costing requirements

Assignment of personnel and travel expenses

Per-diem and overnight accommodation 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 (downloadable at <https://www.bundesfinanzministerium.de>).

Accommodation costs which exceed this up to a reasonable amount and the cost of flights and other main forms of transport can be reimbursed against evidence

All business travel must be agreed in advance by the officer responsible for the project.

Sustainability aspects for travel

GIZ would like to reduce greenhouse gas emissions (CO₂ emissions) caused by travel. When preparing your tender, please incorporate options for reducing emissions, such as selecting the lowest-emission booking class (economy) and using means of transport, airlines and flight routes with a higher CO₂ efficiency. For short distances, travel by train (second class) or e-mobility should be the preferred option.

If they cannot be avoided, CO₂ emissions caused by air travel should 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 \(German only\)](#) has published a [list of standards \(German only\)](#). GIZ recommends using the standards specified there.

Specification of inputs

Fee days	Number of experts	Number of days per expert	Total	Comments
Designation of Team Lead/ Cybersecurity and SME Capacity-Building Expert	1	30	30	
Designation of Communications and Media Campaign Expert	1	20	20	
Transport	Quantity	Number per experts / Persons	Total	Comments
Car Rental, Fuel and/or Transportation	1	2	Market Rate	Cost of transportation for activities of the consultants
Other costs	Quantity	Price	Total	Comments
Workshops	8	-	Market Rate	Workshops should include cost of the following: 1. Training and communication materials development workshops • 4-day workshop venue • Catering • Workshop materials 2. SME Trainings • 2-day workshops for 35 people (1 cohort) 3. Intermediary Institution Training • 2-day Training of Trainer workshop for 15 staff of intermediary institutions
Accommodation	63	-	Market Rate	Including accommodation for consultants, CSA and DPC staff/representative; at a rate not exceeding GHS 650 per person per night.

Per Diem for Participants	50	GHS 200	GHS 10,000	Per Diems for workshop participants (35 SMEs; 15 staffs of intermediary institutions)
Media campaign & branding materials	1	GHS 78,479	GHS 78,479	Production media: • Radio jingles including translations from English to local languages (Ewe and Twi) • Banners, posters, information materials/fact sheets • Radio airtime; digital and social media • Rental of public address systems
Ground mobilization	2	GHS 500	GHS 1000	Per diem for local points of contact in selected district for mobilisation (2 people)
Transportation- Partners	1	GHS 4500	GHS 4,500	GHS 900 per head as transportation for 5 partners (4 from CSA and 1 from DPC) from Accra to Volta Region as well as return to Accra
Communication	1	-	Market Rate	Lumpsum for phone airtime, internet, stationery, printing of questionnaires, photography, renting of recorders etc.)
Flexible remuneration	1	-	GHS 17,723	A budget of GHS 17,723 for foreseen flexible remuneration. Please incorporate this budget into the price schedule. <i>Use of the flexible remuneration item requires prior written approval from GIZ.</i>

6. 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 (language).

The complete tender must not exceed 15 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 (language).

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.