FINNISH DIGITAL & GREEN TRANSITION

18 September 2026

Terms of Reference for Short-Term Expert(s) Providing Capacity Building in the Assessment of Telecommunications Network Vulnerabilities and Resilience in the Dominican Republic

Organisation: HAUS Finnish Institute of Public Management Ltd

Project: Finnish Digital and Green Transition (FDGT)

Host Organisation: The National Cybersecurity Center of the Dominican Republic (CNCS)

1. Purpose of the Document

This Terms of Reference defines the requirements for procuring a Short-Term Expert (STE), or a team of up to two complementary STEs, to support the National Cybersecurity Center of the Dominican Republic (CNCS) in assessing vulnerabilities and resilience within the country's telecommunications environment.

The assignment is implemented under the Finnish Digital and Green Transition (FDGT) project, which deploys Finnish expertise through targeted secondments to support human-centred digital transformation in partner countries.

The assignment will combine a practical, risk-based assessment with institutional capacity building. It will identify and prioritise vulnerabilities, risks and capability gaps; develop actionable recommendations to strengthen telecommunications security, resilience and operational continuity; and strengthen national capacity to conduct future assessments and manage related risks.

The Client (HAUS Finnish Institute of Public Management Ltd) reserves all rights to amend, modify, edit, update and withdraw this document and the information contained herein.

2. Background

Finnish Digital and Green Transition Project (FDGT)

The goal of the FDGT project (2025-2027) is to promote human-centred digital development in Africa, Asia and Latin America in partnership with Finland. The FDGT project focuses on:

- Offering short-term secondments whereby experts from Finland are sent to work in public organisations in Africa, Asia and Latin America for up to 6 months. Secondment is a means to support Digital and Green Transition in these regions by offering technical

assistance based on Finnish good practices in digitalisation, while having a unique chance to forge partnerships with local stakeholders.

- Supporting the introduction of Finnish expertise and digital concepts to various international initiatives, including Team Europe Initiatives under the EU Global Gateway strategy to respond to the needs in Africa, Asia, Latin America and the Caribbean.
- Providing high-quality and timely expert services for the coordination of the EU and its Member States work in promoting human-centred digital development in the Digital for Development (D4D) Hub in Brussels.

FDGT is a **development cooperation project** funded by the **Finnish Ministry of Foreign Affairs** and implemented by **HAUS**.

3. Context and Host Organisation

The STE(s) will be procured and seconded to the following organisation: **The National Cybersecurity Center of the Dominican Republic (CNCS)**

Context

Identified Need and Opportunity

The Dominican Republic's telecommunications infrastructure is a critical enabler of public services, economic activity, digitalisation and national security. Growing dependence on digital connectivity, increasingly interconnected infrastructure and an evolving cyber threat landscape place greater demands on telecommunications security, resilience and operational continuity.

The Dominican Republic has identified a need to strengthen its technical and methodological capacity to systematically assess vulnerabilities and risks across this environment. This includes developing a clearer understanding of technical and operational vulnerabilities, dependencies and capability gaps; their potential impact on critical services; and appropriate measures to mitigate them in accordance with recognised international standards and good practices.

The secondment will respond to this need through a practical, risk-based vulnerability and resilience assessment combined with institutional capacity building. The assignment is intended to produce an evidence base for prioritising improvements and future investments while transferring methodologies and expertise that enable CNCS and relevant national stakeholders to strengthen their capacity for future assessments and risk management.

The findings may also identify areas where further international cooperation, specialised expertise, training, pilots, research and innovation cooperation, or technical solutions could support implementation. Where relevant, this may include opportunities to draw on Finnish

expertise and capabilities, while maintaining technology and vendor neutrality and without predetermining future procurement decisions.

Host Organisation

Organisational Overview

The National Cybersecurity Center of the Dominican Republic (CNCS) is the national entity responsible for coordinating and strengthening cybersecurity management and supporting the protection of the country's critical information and telecommunications infrastructure. It plays a central role in national cybersecurity coordination, incident prevention and response, and cooperation between relevant public- and private-sector actors.

CNCS will act as the host organisation and principal technical counterpart for the secondment. It will coordinate access to relevant institutions and stakeholders, facilitate the assessment, support validation of findings and help ensure that recommendations are aligned with national priorities.

CNCS's operational structure includes the Cybersecurity Strategy Coordination Team (ECEC), responsible for coordinating national cybersecurity policies, strategies and related projects; the National Cyber Incident Response Team (CSIRT-RD), which supports responses to cyber incidents affecting critical infrastructure and State information systems; and the Security Operations Center (SOC), which provides monitoring and operational visibility supporting the protection of public-sector digital assets.

Strategic Framework

The secondment forms part of the Dominican Republic's wider efforts to strengthen cybersecurity, digital infrastructure and the resilience of critical services. It supports national priorities related to risk management, incident prevention, critical infrastructure protection, operational continuity and the development of specialised cybersecurity capacities.

The vulnerability and resilience assessment will provide technical evidence to support these priorities and inform longer-term national capability development and investment planning.

Existing Digital Capabilities

CNCS already uses specialised digital technologies to support cybersecurity monitoring, threat detection, vulnerability analysis, incident management, security-event correlation, information management and coordination with other institutions.

The secondment will build on these capabilities rather than seek to replace them. Where gaps are identified, the assessment should distinguish between improvements that can be achieved

through processes, capacity building or better use of existing capabilities and those that may require additional technical capabilities, specialised services or future investment.

Stakeholder Landscape

The assignment will require close engagement with stakeholders responsible for cybersecurity, telecommunications, digital government, critical infrastructure and national security. Key stakeholders include:

- Government Office of Information and Communication Technologies (OGTIC);
- Dominican Institute of Telecommunications (INDOTEL);
- Ministry of Industry, Trade and MSMEs (MICM);
- Ministry of Interior and Police (MIP);
- National Intelligence Directorate (DNI) and other relevant national security bodies;
- private telecommunications operators and service providers;
- academic institutions and research centres active in ICT and cybersecurity;
- relevant private-sector technology and cybersecurity actors; and
- Finnish stakeholders where relevant to needs identified through the assignment.

Engagement with telecommunications operators and other relevant private-sector actors will be particularly important for developing a realistic understanding of vulnerabilities, operational constraints and existing capabilities.

Daily Work of the Seconded Expert(s)

The STE(s) will be embedded within CNCS and work closely with its strategic and operational cybersecurity functions and relevant external stakeholders.

The work will be practical and collaborative, with the assessment undertaken jointly with Dominican counterparts to support knowledge transfer and strengthen their capacity to conduct future assessments and manage related risks. The activities will follow the methodology and assessment process described in Section 5.

Collaborating units:

- Cybersecurity Strategy Area;
- Incident Management Operational Area;
- Legal Area;
- International Cooperation Area; and
- Computer Crime Investigation Division (DIDI) of the National Intelligence Directorate (DNI).

The STE(s) will also engage with other public authorities, telecommunications operators, technical experts, academic institutions, and private-sector stakeholders where required for the assessment.

Workplace: The primary workplace will be the offices of the National Cybersecurity Center (CNCS) in Santo Domingo, Dominican Republic. The assignment may also include visits to relevant institutions and telecommunications stakeholders, complemented by remote work where appropriate.

Focal points:

- Carlos Leonardo, Executive Director, National Cybersecurity Center (CNCS);
- Angela Noelia Martinez, Director of Strategy Coordination, CNCS;
- Yahaira Abreu, Coordinator of Cooperation and Interinstitutional Relations, CNCS; and
- Armando Díaz, Head of the Computer Crime Investigation Department (DIDI).

The focal points will support the STE(s)' institutional integration, facilitate access to relevant technical counterparts and stakeholders, coordinate information exchange and meetings, and support the validation and follow-up of the secondment's findings and recommendations.

4. Objectives of the Secondment

Main Purpose

To support the National Cybersecurity Center of the Dominican Republic in assessing vulnerabilities and resilience within the telecommunications environment, strengthening national technical capacity and supporting the protection and operational continuity of critical telecommunications infrastructure.

Specific Objectives

The secondment aims to:

- conduct a practical, risk-based assessment of selected vulnerabilities, risks and dependencies within the telecommunications environment;
- identify and prioritise technical, operational and institutional capability gaps;
- develop actionable recommendations to strengthen telecommunications security, resilience and operational continuity;
- strengthen the capacity of CNCS and relevant stakeholders through joint assessment, knowledge transfer and specialised methodologies; and
- identify priority areas for follow-up measures, future investment and, where relevant, continued Dominican–Finnish cooperation.

5. Methodology and Approach

The assignment will undertake a **risk-based, non-intrusive assessment of selected critical components, dependencies, cybersecurity arrangements, and resilience capabilities within the Dominican Republic's telecommunications ecosystem**. The purpose is not to conduct an exhaustive technical audit or penetration test of the entire national telecommunications network, but to identify systemic vulnerabilities, priority risks, capability gaps, and practical opportunities for strengthening national telecommunications resilience.

The detailed assessment scope will be agreed during an inception phase between the STE(s), CNCS, HAUS and relevant national stakeholders, taking into account the criticality of infrastructure, availability of information, stakeholder participation, security and confidentiality requirements, and the time available for the assignment.

Given the scale and complexity of the national telecommunications environment, the assessment is not expected to cover all networks, systems, operators or technical controls comprehensively. Tenderers should propose a risk-based approach for selecting and prioritising the infrastructure, stakeholders, technical areas and controls to be assessed within the available timeframe. The final assessment scope and sample will be agreed with CNCS.

Assessment areas

The assessment is expected to cover the following four dimensions:

1. Critical telecommunications infrastructure and dependencies

Develop a high-level understanding of the telecommunications ecosystem relevant to national resilience, including selected critical infrastructure, services, dependencies, interconnections and potential concentration or single points of failure. The assessment will draw on available documentation, stakeholder interviews and information provided by relevant authorities and participating telecommunications operators.

2. Cybersecurity and technical controls

Assess selected cybersecurity arrangements and technical controls relevant to telecommunications resilience. Depending on the systems and information made available, this may include network architecture and segmentation, access control, security monitoring, vulnerability and patch management, configuration and hardening practices, incident detection and response, redundancy and recovery arrangements, and relevant third-party or supply-chain dependencies.

Technical assessment activities shall primarily be non-intrusive. Any assessment requiring access to operational systems or sensitive technical information shall be separately agreed with the relevant system or infrastructure owner.

3. Operational resilience and institutional preparedness

Assess the arrangements for preventing, managing and recovering from significant cybersecurity incidents or disruptions affecting telecommunications services. This should include relevant coordination and information-sharing arrangements between CNCS, CSIRT-RD, telecommunications authorities, operators and other key stakeholders, as well as incident escalation, continuity arrangements, crisis preparedness and opportunities for joint exercises or other forms of operational testing.

4. Capability gaps and development needs

Based on the assessment, identify and prioritise gaps according to their potential impact and urgency and distinguish, where feasible, between:

- gaps that can primarily be addressed through organisational processes, governance or capacity building;
- gaps that can be addressed through improved use or configuration of existing capabilities; and
- gaps that may require additional technical capabilities, specialised services or future investment.

For identified development needs, the STE(s) should describe relevant functional requirements and possible implementation pathways without prescribing individual vendors or procurement solutions.

Assessment process

The assignment is expected to proceed through the following stages:

Inception and scoping: Confirm assessment boundaries, priority infrastructure and stakeholders, information requirements, assessment criteria and applicable international standards or good practices.

Evidence collection and stakeholder engagement: Review relevant documentation and conduct structured interviews, workshops and consultations with CNCS, relevant authorities, telecommunications operators and other stakeholders.

Targeted technical assessment: Conduct agreed non-intrusive assessments of selected technical environments, controls and operational arrangements. The precise technical activities will depend on access and authorisation provided by participating organisations.

Risk and gap analysis: Analyse identified vulnerabilities and capability gaps using an agreed risk-based methodology and prioritise findings according to criticality, potential impact and feasibility of mitigation.

Validation and capacity building: Validate findings with relevant stakeholders and transfer the assessment methodology and relevant tools or approaches to CNCS and other participating national experts.

Recommendations and roadmap: Develop prioritised recommendations covering immediate improvements, medium-term capability development and potential longer-term investments.

Follow-on cooperation: Identify areas in which further international cooperation, specialised expertise, pilot activities, research and innovation cooperation, or technical solutions could support implementation. Where relevant, identify areas in which Finnish expertise and capabilities may be applicable, while maintaining technology and vendor neutrality.

Division of responsibilities:

STE:

- Design and application of the methodology
- Technical analysis
- Preparation of reports and recommendations
- Facilitation of workshops and training sessions

Host Organization:

- Institutional coordination
- Facilitating access to information and key actors
- Technical and strategic validation of results

6. Expected Deliverables

- **Telecommunications Network Vulnerability Diagnostic Report**
- **Document of prioritized technical recommendations**
- **Roadmap for capacity building**
- **Training materials** (presentations and guides)
- **Report on opportunities for future cooperation**
- **A presentation of the main findings and achievements** of the secondment to the host organisation, HAUS, the Finnish Ministry of Foreign Affairs and the Finnish Embassy.

- **Final report on the mission including:** Description of the activities carried out; Contribution of activities to achieve the above-mentioned objectives; Assessment of the potential for continued cooperation between Finnish actors and the partner organisation, and; Lessons learned, including recommendations for possible future temporary commissions.

7. Duration and Timeline

Planned Timing: The assignment is expected to commence in **January 2027.** The exact start date shall be confirmed in coordination with STE(s) and the host organisation.

Duration: The secondment shall have a maximum duration of **120 person-days.** The maximum of 120 person-days applies to the combined input of all proposed experts and backstopping personnel.

The assignment may be delivered through a combination of on-site and remote work; however, **no more than 30% of the total input may be provided remotely (including possible backstopping)**.

Tentative timeline:

Period	Activities	Deliverables
Weeks 1–2	**Inception and scoping:** confirm assessment boundaries, priority infrastructure and stakeholders, information requirements, assessment criteria and applicable	Agreed assessment scope and work plan
Weeks 3-7	**Evidence collection and stakeholder engagement:** document review, structured interviews, workshops and consultations with CNCS, authorities, operators and other stakeholders	Stakeholder consultations and initial capacity-building workshop
Weeks 8-13	**Targeted technical assessment and practical knowledge transfer:** agreed non-intrusive assessments of selected technical environments, controls and operational arrangements across the four assessment areas. Where feasible, undertake activities jointly with CNCS and participating experts, complemented by practical technical sessions.	Technical assessment findings and practical knowledge-transfer sessions

Weeks 14-17	**Risk and gap analysis:** analyse identified vulnerabilities and capability gaps, prioritise findings by criticality, impact and feasibility	Draft Telecommunications Network Vulnerability Diagnostic Report
Weeks 18-20	**Validation and capacity building:** validate findings with stakeholders, transfer assessment methodology and tools to CNCS and participating experts	Training materials; finalised Diagnostic Report
Weeks 21-22	**Recommendations and roadmap:** develop prioritised recommendations covering immediate, medium-term and longer-term measures	Document of prioritised technical recommendations; Roadmap for capacity building
Weeks 23-24	**Follow-on cooperation and closure:** identify areas for further cooperation, including Finnish expertise; finalise and present findings	Report on opportunities for future cooperation; Presentation of main findings; Final mission report

Evaluation note:

- When evaluating tenders, proposals that allocate a greater number of person-days (up to the maximum of 120) will be viewed favourably, as this indicates stronger capacity to deliver the full scope and outputs of the assignment. The score for person-days will be calculated proportionally using the following formula: **Person-days score = (Proposed person-days / 120) × maximum score.** Proposals offering 120 person-days will receive the full score, while lower allocations will receive proportionally fewer points.

- **Certain tasks may be conducted remotely where this is duly justified, up to a maximum of 30% of the total input.** Remote work may be particularly suitable for analytical and drafting tasks, including risk and gap analysis and the development of recommendations and the roadmap.

  However, given the nature of the assignment, a strong on-site presence is considered to add value throughout the secondment by enabling closer collaboration with CNCS and other stakeholders, facilitating access to relevant information, strengthening knowledge transfer, and allowing the experts to respond flexibly to emerging assessment needs. Stakeholder engagement, technical assessment, validation and capacity-building activities are therefore expected to be delivered primarily on-site.

  Accordingly, proposals with a higher proportion of on-site work will receive a higher score for delivery modality. The score will be calculated proportionally as follows:

  On-site score = (On-site person-days / total person-days) × maximum score

A proposal with 100% on-site input will receive the maximum score for this criterion. Proposals including remote input will receive a proportionally lower score, provided that remote input does not exceed 30% of the total person-days.

8. Budget and Payment

In the Budget Form (Appendix A), the tender shall include the proposed daily remuneration rate (item 1 below). **The same rate shall apply to all proposed input, including all expert input and organisational backstopping.** All other costs listed below (items 2–5) are covered by HAUS and shall not be included in the Budget Form

1. **Daily remuneration (to be proposed by the tenderer)**
2. International per diem allowance
3. Travel expenses to and from the assignment location
4. Accommodation expenses
5. Operational budget for local expenditure such as visa, phone contract, internet, workshops, translation and interpretation etc (to be determined on a case-by-case basis)

The terms of compensation follow the Finnish Government's travel expense reimbursement guidelines, and the conditions set out in the Contract.

Payment will be made monthly, based on actual workdays completed and receipts for the reimbursable expenses listed above.

9. Expert Resourcing and Qualifications

The assignment may be delivered either by **one expert** covering all required areas of expertise, or by **two complementary experts** with clearly defined and jointly responsible roles. In the case of two experts, one shall act as **Lead Expert/Coordinator,** responsible for overall coherence, strategic direction and stakeholder engagement, while the **second expert focuses on specific thematic or technical areas** as defined in the tender.

The Lead Expert is expected to demonstrate strong capability in stakeholder coordination, institutional engagement, delivery oversight, and integration of outputs. Deep technical specialization in all technical domains is not required for the Lead Expert, provided these competencies are adequately covered by the supporting expert. The proposed allocation of responsibilities and person-days between the two experts shall reflect their respective roles and the expertise they are expected to contribute to the assignment.

Additionally, both delivery models may include **organisational backstopping support** from the experts' home organisation for specific technical, sectoral or commercial expertise.

Backstopping may support, for example, **specialised analysis, methodological advice, quality assurance, review of findings and deliverables, and other clearly defined expert inputs that can appropriately be provided remotely**. It shall complement, and not replace, the Lead/Sole Expert or Second Expert in the core implementation of the assignment.

Any backstopping must be **clearly defined in the Technical Form (Appendix C)**, including the **name of each backstopping expert, area of expertise, specific activities or deliverables supported, and allocated person-days**. A maximum of **two backstopping experts** may be proposed. Organisational backstopping is limited to **15 person-days in total**, must be included within the overall ceiling of 120 person-days, and shall be delivered entirely remotely.

CVs (maximum 3 pages each) of all proposed experts, including potential backstopping experts, must be included in the tender documentation.

Qualifications

- **Public-Sector Cybersecurity & Critical Infrastructure Experience (Max 20 points)**

  Experience supporting public-sector or critical-infrastructure organisations, including telecommunications, in assessing and strengthening cybersecurity, resilience and operational continuity through risk-based assessments, institutional process development, mentoring and operational support.

  Relevant experience may include vulnerability or risk assessments of telecommunications or other critical infrastructure, application of relevant international standards and frameworks (e.g. ISO/IEC 27001, NIST Cybersecurity Framework, or ITU-T/ENISA telecommunications security guidance), and coordination with regulators, operators and national cybersecurity authorities.

  Experience should demonstrate practical assessment and institutional strengthening work rather than exclusively high-level policy or strategy design.

- **Practical Technical Expertise in Telecommunications and Cybersecurity (Max 20 points)**

  Demonstrated hands-on experience in one or more of the following areas:

  - Telecommunications network architecture, segmentation and resilience, including redundancy and recovery arrangements
  - Vulnerability and risk assessment methodologies, including non-intrusive technical evaluation
  - Security monitoring, access control, and incident detection and response
  - Critical infrastructure protection and third-party or supply-chain risk
  - Configuration, hardening, and vulnerability and patch management practices

  Experience should demonstrate practical technical assessment capability relevant to a risk-based diagnostic of national telecommunications infrastructure.

- **Operational Assessment, Diagnostic & Delivery Capability (Max 15 points)**

  Demonstrated experience designing and delivering vulnerability or risk assessments, diagnostic studies, or resilience reviews within public-sector or complex institutional environments, translating technical findings into prioritised, actionable recommendations.

  Relevant experience may include developing risk registers, gap analyses, capability roadmaps, or structured diagnostic reports in cybersecurity, telecommunications or critical infrastructure contexts.

  The focus is on demonstrated ability to deliver feasible, evidence-based outputs, such as diagnostic reports, prioritised recommendations and roadmaps, that can be adopted within institutional settings, rather than purely conceptual design.

- **Facilitation (Max 15 points)**

  Demonstrated experience in designing and delivering capacity-building activities in complex institutional environments, particularly within public-sector digital transformation or cybersecurity contexts.

  Relevant experience includes delivering training, workshops, simulation exercises (e.g. incident response drills), mentoring programs, and structured knowledge transfer activities aimed at improving institutional capabilities in cybersecurity and infrastructure resilience.

  The expert should also demonstrate strong stakeholder engagement and facilitation skills, including the ability to work effectively with technical teams, senior management, and external stakeholders in multidisciplinary and cross-cultural environments. This includes the ability to communicate complex technical or cybersecurity concepts in an accessible and operationally relevant manner.

  The focus is on practical capability transfer, institutional learning, and stakeholder alignment that leads to sustained operational improvement, rather than one-off training delivery or academic instructions

- **Emerging Market Experience (5 points)**

  Proven experience working in emerging market contexts, preferably in cybersecurity, telecommunications, or critical digital infrastructure.

- **Education (3 points)**

University degree in Engineering, Telecommunications, Cybersecurity, Information Systems, Computer Science, Public Policy, or a closely related field.

- **Language (8 points)**
  - Full professional written and spoken fluency in English is required for eligibility (see Eligibility criteria) and is scored up to 3 points in this component.
  - Working or professional proficiency in Spanish is considered an additional asset, given its role as the primary working language of most host-organisation stakeholders and telecommunications sector counterparts, and is scored up to 5 points.

10. Evaluation

The selection of the seconded expert(s) will be based on a combined **quality and price assessment**. The quality assessment will have the predominant weight to ensure the selection of a highly qualified expert(s).

	QUALITY 80% **The raw quality score is 106 points (Expert Form 86 + Technical Form 20), which is converted to a weighted score of 80 points.**
Basic Information	The quality assessment will account for 80% of the overall evaluation. It will be based on the information provided in: • the **Expert Form (Appendix B)**, • the **Technical Form (Appendix C, note max 10 pages)**, and • **Expert CV(s)** (supporting document; **maximum 3 pages per CV**).
Interviews	The Contracting Authority reserves the right to conduct structured interviews with the two (2) to four (4) highest-ranked tenderers following the preliminary written evaluation. The purpose of the interview is to: • Verify information provided in the tender • Assess spoken English proficiency and communication skills • Clarify specific aspects of the expert's experience or methodology where necessary The interview will relate only to evaluation criteria already defined in this ToR. Not all criteria must be revisited during the interview. Based on the interview, provisional quality scores may be confirmed or adjusted where justified. The number of tenderers invited to interview will be determined based on the distribution of preliminary quality scores.

Expert Form (Appendix B)	Each criterion listed under the *Required Expertise* section in this ToR will be scored up to the maximum points allocated to that criterion - according to the depth and relevance of the candidates' experience, as demonstrated in the Expert Form, and relevant CV(s), as applicable to the proposed resourcing model. ***(Total score: 86 points)*** The CV(s) should be concise, up-to-date supporting document(s) (maximum 3 pages each), highlighting relevant experience that complement the Expert Form.
Two-expert proposals	Tenders may propose either **one expert covering all required areas of expertise** or **two experts whose combined qualifications fulfil the requirements**. Each proposed expert will be scored individually against the published criteria. For two-expert tenders, the team score for each criterion will normally be based on the higher of the two individual expert scores ("best-of-two" principle). **An expert's experience may be taken into account for a criterion only where the expert has a substantive role and sufficient input in the relevant activities or deliverables.** Tenderers shall clearly specify each expert's responsibilities, deliverables and number of person-days in the Technical Form.
Backstopping	Backstopping experts are not scored as separate experts. Where the ToR permits specialised backstopping expertise to complement the proposed expert(s), it may be considered in assessing coverage of the relevant criterion. Its contribution and person-days must be demonstrated in the Technical Form.
Technical Form (Appendix C)	The Technical Form (maximum 10 pages) covers key qualitative and quantitative aspects of the tender and each of them will be scored up to the maximum points allocated to that criterion. The form covers: Understanding and scope justification (5 points), Proposed approach and methods (5 points), Number of person-days (2,5 points) and on-site/remote allocation (2,5 points), and Delivery modality (including the single-expert-plus-backstopping model or, if proposed, a two-expert model, and any backstopping arrangements) (5 points). ***(Total score: 20 points).***
Minimum quality requirements	To be considered for contract award, **tenders must achieve a minimum of 60% of the total quality score.** Tenders failing to meet this threshold will not be considered for contract award.

Total quality score	Expert Form (Appendix B) 86 points + Technical Form (Appendix C) 20 points = 106 points Converted into a weighted value of 80% **Weighted Quality Score = (Tender Quality Score / Maximum Quality Score) × 80**

Indicative scale for qualitative evaluation criteria

The quality scores will be assigned based on the following indicative scale. The scale shall be applied to each qualitative evaluation criterion in light of the specific requirements of that criterion and the evidence requested in the relevant tender document. Evaluators shall consider, as applicable, the relevance, depth, specificity, credibility and completeness of the evidence provided, as well as its linkage to the assignment, required tasks and expected outputs.

Score range	Description
0–20% of max points	**Very weak:** The criterion is not addressed, or the information provided is largely irrelevant or unsupported. Required elements are missing or there is insufficient evidence to establish the tenderer's capability or suitability in relation to the criterion.
21–40%	**Weak:** The criterion is addressed only partially. Some relevant evidence is provided, but important elements are missing, insufficiently developed, weakly substantiated or only indirectly relevant to the assignment. Significant weaknesses or delivery risks remain.
41–60%	**Satisfactory:** The criterion is addressed to an acceptable level and the proposal demonstrates generally relevant capability, experience or approach. However, the evidence lacks depth, specificity, direct comparability or sufficient linkage to the assignment, tasks and expected outputs.
61–80%	**Good:** The criterion is addressed clearly and comprehensively. The proposal provides relevant and credible evidence, demonstrates a good understanding of the assignment and/or strong relevant capability, and establishes clear links to the required tasks and outputs. Any weaknesses are minor and do not materially affect confidence in delivery.
81–100%	**Excellent:** The criterion is addressed fully and convincingly, with highly relevant, specific and well-substantiated evidence. The proposal demonstrates substantial depth, strong understanding and/or proven capability directly applicable to the assignment, with clear responsibilities, results and links to the required outputs. No significant weaknesses are identified.

	PRICE 20%
Basic information	The tenderer shall indicate the **proposed daily remuneration rate** in the Budget Form (Appendix A). For the price assessment, only the daily remuneration rate will be compared across tenders, not the total price. The lowest rate receives the highest score (20 points). Other tenders will receive proportionally lower scores according to the ratio of their proposed rate to the lowest rate. The same daily rate shall apply for all services. **Price Score = (Lowest Tender Price / Tender Price Being Evaluated) × 20**

11. Eligibility Criteria

Eligibility criteria ensure that only qualified tenderers are considered, while evaluation criteria determine the quality and suitability of tenders. The required experience must be demonstrated by the **proposed expert(s) themselves** as part of their professional CVs and assigned roles, and cannot be fulfilled solely through organisational backstopping.

1. The **Lead Expert** must demonstrate a **minimum of 5 years of relevant professional experience** in cybersecurity, telecommunications, critical infrastructure protection, or public-sector digital systems

   In case of a two-expert proposal, the Lead Expert must meet this requirement in full. The **second expert** must demonstrate a **minimum of 3 years of relevant professional experience** in the above fields.

   For the purposes of this requirement, relevant experience refers to hands-on assessment or operational experience in telecommunications network security and critical infrastructure protection, including areas such as network architecture and resilience, vulnerability and risk assessment methodology, incident response and security monitoring, and access control in ICT or telecommunications environments.

2. The proposed expert team must collectively demonstrate proven **practical experience relevant to telecommunications vulnerability assessment and critical infrastructure** protection to ensure effective delivery of the assignment. This shall include demonstrated experience in *at least two* of the following areas:
   a. Telecommunications network architecture, segmentation and resilience
   b. Vulnerability and risk assessment methodology, including non-intrusive technical evaluation

   c. Incident response and security monitoring
   d. Critical infrastructure protection and supply-chain risk
   e. Access control and technical security controls in ICT or telecommunications environments
   f. In case of a two-expert proposal, these competencies may be distributed across the proposed experts.
3. The service provider is required to be a **Finnish legal entity** or other entity which has a **Finnish Business ID**
   a. This requirement reflects the mandate of the FDGT project to mobilise Finnish expertise and support cooperation between partner institutions and the Finnish digital ecosystem.
4. The expert must be **fluent in English** (speaking and writing), with excellent drafting, analytical, and communication skills.
5. The tender includes all required documents: **Budget form (Appendix A), Expert form (Appendix B), CVs, and Technical Form (Appendix C).**
6. Full compliance with relevant data protection regulations, including GDPR, and adherence to the Principles of Conduct Clause outlined in this ToR.

12. Tender Submission Details

All proposals must be submitted electronically through the tender portal.

The tender must demonstrate that the service provider meets the **eligibility** criteria. **Only eligible candidates will be considered**.

Requested documents are:

- Budget Form (Appendix A)
- Expert Form (Appendix B)
- CV highlighting relevant experience (**note CV max 3 pages**)
- Technical Form (Appendix C, **note max 10 pages)**

The minimum font size is 11 points. All documentation must be in English.

Tenders will be opened collectively after the submission deadline. Evaluation will then be carried out in accordance with the published criteria. Contracting will proceed following the completion of the evaluation process and the expiry of the appeal period.

Personal data contained in the submitted documents will be processed solely for the purposes of this procurement procedure. The documents will be shared with members of the selection panel as part of the evaluation process but will be retained only for as long as necessary for the purposes of this procurement, after which they will be securely deleted in accordance with applicable data protection requirements.

13. Questions during the Procurement

During the procurement process, all interested parties are encouraged to submit any questions or clarifications regarding the procurement process via the online system. All questions received will be addressed as soon as possible. Please ensure that all inquiries are submitted within the specified timeframe indicated in the tender portal to allow for a timely response.

Only communication and contacts made through the Supplier Portal will be considered. The Contracting Authority is unable to respond to queries made otherwise, for example by telephone, mail or e-mail.

14. Reporting

The STE(s) will report to FDGT Project Manager and will maintain regular communication with the FDGT team throughout the secondment.

The STE(s) delivers a timesheet on the actual workdays and hours at the end of each month to the FDGT team.

15. Anti-Corruption

FDGT is committed to preventing and not tolerating any act of corruption and other malpractices and expects that all bidders will adhere to the same ethical principles.

16. Principles of Conduct Clause

Service Provider seeking to work with the Client (HAUS) shall adhere to the following principles:

- **Confidentiality**: Service provider must only use information solely for the purpose of performing their duties with the Client.
- **Business Ethics:** Service Provider are expected to uphold the highest standards of business ethics when collaborating with the Client
- **Transparency of Information Provision:** Service Provider must refrain from engaging in any fraudulent activities or misrepresenting information to influence the selection and contract awarding process in their favour
- **Fair Competition:** Service Provider should abstain from participating in corrupt, collusive, or coercive practices
- **Officials Not to Benefit:** The Service Provider guarantees that no official associated with the Client has received or will receive any direct or indirect benefit from the Bidder, the

Service Contract or its award. Any violation of this provision will be deemed a breach of a fundamental term of the Service Contract

- **Data Protection:** Service Provider must comply with all relevant data protection laws and regulations, ensuring the confidentiality and security of any personal or sensitive data provided during the collaboration.

17. Rights reserved

This RFP does not obligate FDGT to complete the tendering/RFP process.

FDGT reserves the right to amend any segment of the tendering/RFP prior to the announcement of the selected STEs.

FDGT reserves the right to remove one or more of the services from consideration for this contract should the evaluation show that it is in FDGT's best interest to do so.

FDGT may, at its discretion, issue a separate contract for any service or groups of services included in this tendering/RFP.

FDGT may negotiate a compensation package and additional provisions to the contract awarded under this tendering/RFP.

FDGT reserves the right to debrief the tenderers after the completion of the process due to possible high volume of tenders and avoiding the compromise of the process.