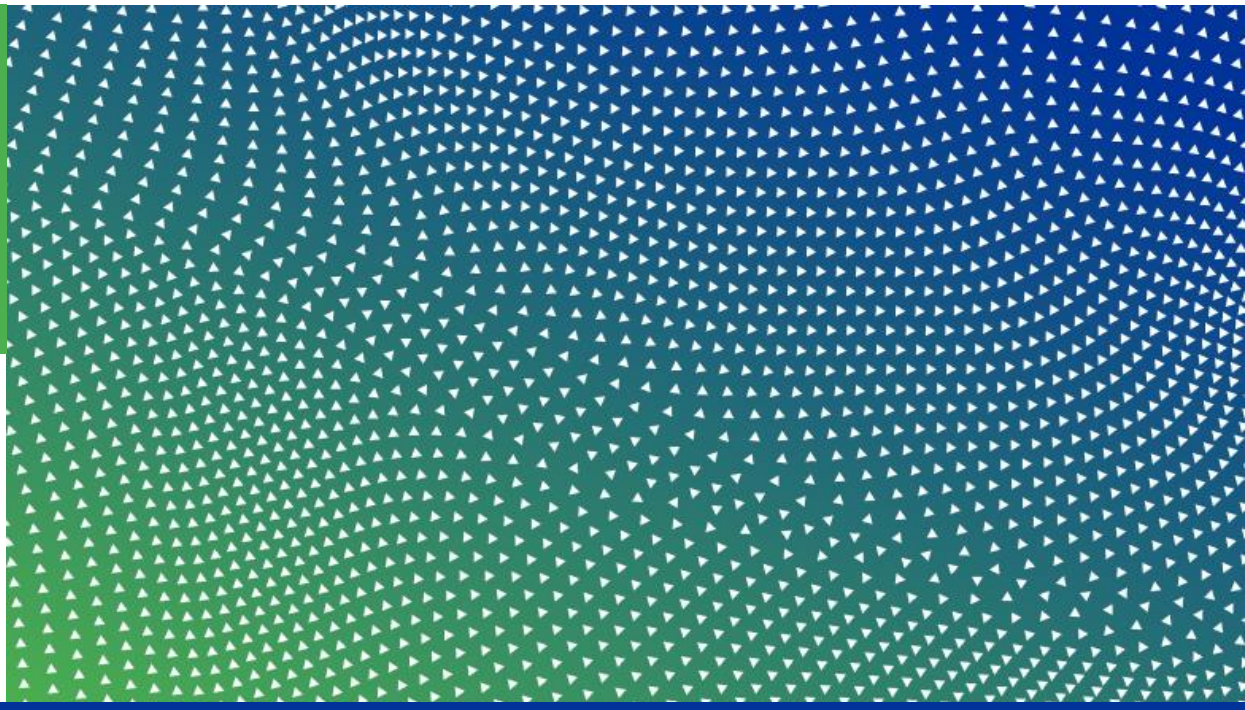
DATA
GOVERNANCE
IN AFRICA



Supporting development-oriented and human-centric data regulation, use and infrastructure in Africa

Terms of Reference for Designing a Secure Data Infrastructure Management Knowledge Stream for Enhanced Organizational Resilience and Security

Digital Investment Facility

Author: Juha Miettinen

30 April 2025

Version: 2.0

Terms of Reference for Designing a Secure Data Infrastructure Management Knowledge Stream

1. Project Overview

HAUS Finnish Institute of Public Management Ltd implements this procurement on behalf of the Digital Investment Facility (DIF), which is part of the broader Data Governance in Africa initiative. The DIF is a joint initiative led by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH and funded by the European Union.

The objective of this Terms of Reference (ToR) is to outline the objectives, scope, deliverables and methodology for developing practical guidelines and training material for secure data infrastructure [1] management for the DIF knowledge provision and dissemination. The knowledge package should support in creating more enabling environment via capacitating infrastructure (e.g. datacentre and IXP) developers and promoters to apply practices for the establishment and management of a secure and trusted data centre infrastructure. A special emphasis is on cybersecurity; in an era of increasing cyber threats, this framework aims to protect sensitive data, maintain operational integrity, and ensure compliance with applicable regulations. E.g. The EU toolbox for 5G security could be utilised as a source in designing the guidelines. A seasoned consultant team will be procured to execute the preparation of the package under supervision of the DIF team.

2. Background and rationale

In today's data-driven environment, secure and efficient data infrastructure is essential to support decision-making, operations, and long-term growth. There is an evident need for support in physical security and cybersecurity issues of data infrastructure. In many African countries facilities hosting data infrastructure have faced violence, crimes and cybersecurity breaches with severe consequences that led to reputational damage and financial loss. Capacity to ensure safety and cybersecurity of data infrastructure is a critical factor e.g. in the planning and operation of data centres. To support stakeholders' capacities and project design, technical guidelines on secure data infrastructure needs to be developed. The guidelines and training material thereof aim to ensure a smooth and uninterrupted data flow and that in the facilities data is stored, processed, and retrieved within a framework that maintains confidentiality, integrity, and availability, aligned with best practices and regulatory requirements.

[1] Data infrastructure here refers to several possible segments ranging from 1) First mile like optic fibre used for submarine cable or terrestrial backbone (country/regional/transcontinental link); 2) Mobile network coverage using 4G /5G technology or dedicated network link to connect distribution point; 3) data centre and exchange node (IXP); 4) Tower companies sharing passive and active infrastructure; 5) TESCo/ESCO as solar farm or dedicated private power companies; 6) Last mile optical fibre or wireless with 4/5G technology or dedicated microwave or satellite link.

In the European Union securing these digital infrastructures is essential to protect both national security and individual privacy. Recognizing these challenges, the EU has introduced the 5G Toolbox as a framework to ensure secure, resilient, and trusted telecommunications and IT infrastructures. The toolbox emphasizes risk assessment, vendor trustworthiness, and cybersecurity measures that executors can apply to safeguard critical networks and data centres.

A robust and comprehensive knowledge package on secure data infrastructure management is vital to equip the organizations with the skills and insights needed to protect against vulnerabilities, optimize data workflows, and meet regulatory compliance standards. This initiative will provide a structured approach to managing and securing data assets, promoting organizational resilience and data governance maturity.

With the knowledge package guidelines and training material organisations can

- Strengthen data security by implementing best practices and frameworks for secure data storage, access management, and protection from security and cyber threats
- Improve data infrastructure management by equipping teams with tools and strategies to optimize and maintain the organization's data infrastructure
- Enhance compliance and risk management by ensuring alignment with relevant data protection regulations and minimizing security risks
- Build internal capacity by developing internal expertise and skills on infrastructure management and precautionary measures
- Equip public practitioners with an overview and dimension to consider securing and ensuring trusted vendors are selected for critical digital infrastructure from a regulatory standpoint.

Primary beneficiaries of this knowledge package include the IT, data management, compliance, and risk management units. Stakeholders may also include executive management, as secure and efficient data infrastructure aligns with broader organizational risk management and operational goals. In addition, representatives of national public authorities designed to ensure network and data security may also benefit.

The DIF is supporting the development of secure and resilient data infrastructure in Africa as part of the broader Data Governance in Africa Action, a 3.5-year initiative. This program is aligned with the AU-EU strategic partnership, fostering a human-centric and development-oriented data economy in Africa. Secure digital infrastructure is critical to achieving the objectives of sustainable economic growth, operational resilience, and trusted data governance.

3. Objectives

The primary objectives of this assignment are:

- To develop a comprehensive set of cybersecurity guidelines that address the specific needs and challenges faced across digital connectivity asset classes from first to last mile, ensuring alignment with EU standards such as the 5G Toolbox
- To strengthen the cybersecurity capabilities of data centre operators and stakeholders by providing actionable strategies for data protection, risk mitigation, and regulatory compliance

- To enhance resilience and operational continuity by offering best practices and frameworks for managing infrastructure security and responding to emerging threats
- To equip organizations with tools and training materials to foster local capacity and institutionalize cybersecurity practices within their operations
- To provide regular updates on emerging cybersecurity challenges, trends, and regulatory developments to ensure that the guidelines remain relevant and actionable.

4. Scope of Work

The consultant team will undertake the following activities:

1. Cybersecurity Framework Development, a concrete Practitioner's guide
   - Develop a risk-based cybersecurity framework tailored to African digital infrastructure components, e.g. data centres
   - Incorporate principles from the EU 5G Toolbox, focusing on vendor trustworthiness, risk management, and secure network configurations
   - Address identity and access management, encryption standards, and infrastructure hardening.
2. Data Security Guidelines
   - Provide comprehensive best practices for securing sensitive data, including encryption, data flow monitoring, and endpoint security
   - Include detailed protocols for incident detection, response, and recovery.
3. Regulatory Compliance Guidance
   - Ensure the guidelines comply with key frameworks such as GDPR, AU Convention on Cybersecurity, and other applicable local and international standards
   - Provide recommendations on navigating the regulatory landscape in Africa and Latin America and the Carribean.
4. Evaluation and Benchmarking Tools
   - Create tools to assess the current cybersecurity maturity of digital infrastructure assets
   - Develop templates for gap analysis and benchmarking against best practices
   - Compose a digital repository of existing cybersecurity guidelines, instructions, recommendations and policies etc.
5. Capacity Building Materials
   - Design training modules for in-person and online delivery
   - Conduct two pilot training sessions (one in-person, one online) to test and refine the materials.

5. Expected Deliverables

The following deliverables are expected to be produced during the assignment:

1. Inception Report
   - Providing a comprehensive overview of the Cybersecurity knowledge package project, outlining its objectives, scope, and methodology. It will include a detailed

methodologies for designing the guidelines and training material with a brief analysis of the current state of digital infrastructure cybersecurity practices and mechanisms and identifying the key challenges
- Introducing detailed work packages with planned workloads, milestones and schedules
- Initiating the steering and monitoring mechanisms for the project.

2. Cybersecurity Guidelines Document
   - A comprehensive, EU and internationally compliant document outlining strategies, standards, and best practices for securing digital infrastructure like data centres in Africa.

3. Training Materials
   - Customizable training modules for data centre operators and stakeholders.
   - Detailed lesson plans and resources for both in-person and online training sessions.

4. Pilot Training Sessions
   - One in-person session and one online session to test the training materials.

5. Evaluation Tools
   - Summary briefs on feedback from stakeholders and end-users to refine the guidelines and training material
   - Maturity assessment templates and benchmarking tools to assess cybersecurity readiness and progress of the digital infrastructure assets (e.g. data centres)

6. Repository of relevant existing relevant cybersecurity standards, regulations, guidelines, code of conducts, instructions and recommendations etc. to be possibly posted on DIF website.

7. Final report
   - A short report (max 8 pages) documenting the overall execution of the project, possible challenges and strategic recommendations. The final report serves as a reference for stakeholders and inform future initiatives.

6. Methodology and Approach

The service provision could be carried out e.g. using a combination of primary and secondary research, stakeholder consultations, and iterative development processes. The tenderer should present their own vision, ideas and suggestions on the methodologies for implementing the assignment besides the methods listed below.

The methods should include:

1. Research and Analysis
   - Conduct a comprehensive review of existing cybersecurity frameworks, guidelines, and best practices, including the EU 5G Toolbox
   - Analyse case studies of successful digital infrastructure components security implementations in Africa and other regions.

2. Stakeholder Engagement

- Collaborate with DIF, data centre and other digital infrastructure operators, policymakers, and other stakeholders to understand local contexts and challenges
- Conduct preparatory workshops to gather inputs and validate the relevance of proposed guidelines.

3. Guideline Development
   - Draft the cybersecurity guidelines and training materials
   - Refine the content based on feedback from DIF and stakeholders.

4. Training and Capacity Building
   - Develop and deliver training modules, testing their efficacy through pilot sessions
   - Incorporate feedback to improve the training materials.

The tenderer is advised to indicate how the objectives defined in sections Objectives and Scope of Work (tasks to be performed) are to be achieved. In addition, the tenderer should describe the project management system for the service provision.

The tenderer is required to describe the key processes for the services for which it is responsible and create an operational plan or schedule that describes how the services according to Objectives and Scope of Work, are to be provided.

In particular, the tenderer is required to describe the necessary work steps/packages, specifically related to expected deliverables.

The tenderer is required to explain its approach for coordination with the project. In particular, the project management requirements specified in Objectives and Scope of Work (Tasks to be performed by the tenderer) 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 consulting days) and locations of the individual members of the team complete with the allocation of work steps as set out in the schedule. The tenderer is also required to briefly describe its backstopping concept.

7. Expert Resourcing and Qualifications

The tenderer should provide staff who are fit for the objectives described, based on their CVs, the tasks involved, and the qualifications required. CVs of all personnel must be attached to the tender documentation. Experts should have proven experience in relation to cybersecurity aspects of digital infrastructure, preferable with some experience from Africa.

The following key experts must be provided:

Team Leader
- Overall responsibility for the assignment
- Coordinating and ensuring communication with DIF (HAUS), partners and others involved in the project
- Personnel management
- Regular reporting in accordance with jointly agreed deadlines.

Key Expert(s)
- The tenderer shall assign named key experts

- Key experts are experts who are identified by name in the contract. The tenderer is required to describe the necessary roles, workload, work steps and specialty areas for expert(s).

The selected consultant team/service provider should demonstrate the following:

1. Technical Expertise
    - In-depth knowledge of cybersecurity standards and frameworks, including the EU 5G Toolbox
    - Experience in developing and implementing cybersecurity solutions for digital infrastructure like data centres.
2. Regional Experience
    - Proven track record of working in the Global South, preferably Sub-Saharan Africa, with a strong understanding of local contexts and regulatory environments.
3. Training and Capacity Building
    - Expertise in designing and delivering training programs for technical and non-technical audiences.
4. Stakeholder Engagement
    - Ability to collaborate effectively with diverse stakeholders, including government agencies, private sector actors, and development partners.

8. Timeline

The contract period is envisaged to be ca. 9 months. Contract period is planned to start in May 2025 and to end in January 2026. A draft version of the guidelines shall be ready by the end of August 2025 and the final version by the end of October 2025.

In the proposal the tenderer is encouraged to present a realistic timeline, including milestones for the preparation of the guidelines and training materials as well as a tentative schedule and format for the pilot training sessions.

9. Budget

The estimated total budget for this assignment is maximum EUR 250,000 (excluding VAT), which includes:

- Research and development of cybersecurity guidelines
- Design and delivery of training materials and pilot sessions
- Production of evaluation and benchmarking tools
- All travel costs (travel costs will be reimbursed separately, based on receipts submitted after the trip).

A detailed budget breakdown should be provided based on the scope of work (chapter 4) and deliverables expected (chapter 5), including a tentative consulting day allocation and the daily cost.

Service providers must ensure their proposed costs align with the budget provided and include a clear breakdown of expenses for each project component.

All travel costs for service provider staff must be included in the proposed budget and comply with the Finnish Government's travel expense reimbursement guidelines. For details, refer to: Finnish Government's Official Journeys Guidelines.

Service providers are required to include a payment term proposal, indicating whether they accept the Client's (HAUS) proposed terms or suggest alternatives.

The Client proposes the following payment terms, based on milestone delivery:

- 1. payment: 30% of the contract value (excluding travel costs) upon approval of the inception report (2-3 weeks after signing the contract)
- 2. payment: 30% of the contract value (excluding travel costs) upon DIF approval of the draft version of the guidelines
- 3. Payment: 20% of the contract value (excluding travel costs) after the execution of the pilot training sessions
- Final Payment: 20% of the contract value (excluding travel costs) upon DIF approval of the final report.

Travel Reimbursement: Travel costs will be reimbursed separately, based on receipts submitted after the trip.

10. Evaluation Criteria and Processing of Tenders

Comparison will be executed as follows:

QUALITY - maximum points 75

Quality comparison criterion:

- Relevance and feasibility of the proposed methodology and approach – 20 points
- Viability and comprehensiveness of project work plan – 20 points
- Proven track record on similar assignments and experience and qualifications of the proposed team – 25 points
- Demonstrated understanding of local contexts and challenges – 10 points.

PRICE - maximum points 25

The tender with the lowest price receives 25 points. The comparison points for other tenders for the price section are calculated following the formula: price of the tenderer with the lowest price / price to be compared * 25.

Finally, the total price and quality points are added, and the most economically advantageous tender will be chosen. The most economically advantageous tender is the one with the best price-quality ratio (most total points). If two or more tenders have the same number of points, the tender with the most points for track record and team skills will be selected.

The contract award procedure will progress in the following steps:

1. Opening the tenders and evaluation the suitability of the tenderers
2. Verifying that the tenders and the services tendered meet the requirements of the Invitation to tender
3. Comparison of tenders that meet the requirements of the Invitation to Tender
4. Contract award decision and notification
5. Concluding the Contract. This can only take place by signing the Contract.

11. Submission Requirements

Interested consultant teams should submit the following:

- A detailed technical proposal, including methodology, approach and timelines/milestones, risk assessment with mitigation methods and deliverables (max 10 pages).
- 3 key references and examples of similar assignments (max 2 pages)
- A separate, all-inclusive financial proposal with a clear budget breakdown (max 2 pages). The service provider should propose a clearly defined total project cost, including estimated working days, including all costs associated with data collection and primary and secondary research activities, stakeholder consultations, travelling, report and training material preparation and finalisation, execution of the pilot trainings and designing of the benchmarking and evaluation tools. No other costs are to be accepted.
- CVs of key team members, highlighting relevant experience (max 3 pages each team member as an annex).

Proposals written in English language must not exceed 12 pages, excluding expert CVs, which are limited to 3 pages per CV. The maximum page limit includes any possible cover page and table of contents. The minimum font size for proposals is 11 points. All annexes must be clearly labelled and referenced.

Proposals must be submitted electronically in PDF format by 15th May 2025, 12:00 (Finnish Time, EEST), through the tender portal. Possible requested attachments can be sent directly to kilpailutus@haus.fi.

Proposals and CVs exceeding the maximum page limit, late submissions, or incomplete proposals will not be considered.

All bidders must declare any potential conflicts of interest with the Client (HAUS), its affiliates, or its partners. Failure to disclose conflicts may result in disqualification.

12. Questions during the procurement

During the procurement procedure, the tenderers may request additional information by submitting queries and clarifications concerning the procedure using the Supplier Portal. You will also find the answers provided to your questions in the same place. **The question period will remain open until 7th of May 2025.** All questions received will be addressed by 8th of May 2025. Please ensure that all inquiries are submitted within the specified timeframe 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.

13.Attachments from the service provider

The Service Provider is required to provide the following documents as part of this service contract:

- Certificate of Incorporation: Proof of the Service Provider's legal status

- Tax Compliance Status: Documentation demonstrating the Service Provider's compliance with tax regulations
- Financial Statements: Recent financial statements to assess the Service Provider's financial stability
- Project Team CVs: Detailed resumes of key team members assigned to the project.

14.Steering and Reporting

An internal steering group (HAUS, GIZ and consulting company) will be set up by DIF to support and direct the project implementation. The steering group will meet monthly or whenever is needed while the project is in progress. DIF will assign an internal project responsible/ coordinator to manage and to supervise the project execution.

15.Validity

Proposals and quotes must remain valid for 60 days after the date of closing noted above. After, the closing date and time, all proposals received by the DIF become its property.

16.Anti-Corruption

DIF 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.

17.Principles of Conduct Clause

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

- 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.

The contract will follow the applicable general procurement terms and conditions of HAUS kehittämiskeskus Oy. The procurement is conducted in accordance with Finnish public procurement legislation and Directive 2014/24/EU of the European Parliament and of the Council on public procurement. Where relevant, the assignment aligns with the JIT 2025 framework terms or EU PRAG procurement guidelines, as applicable to publicly funded development cooperation projects.

18.Rights reserved

This RFP does not obligate the DIF to complete the tendering/RFP process.
DIF reserves the right to amend any segment of the tendering/RFP prior to the announcement of a selected consultant team.
DIF reserves the right to remove one or more of the services from consideration for this contract should the evaluation show that it is in DIF's best interest to do so.
DIF may, at its discretion, issue a separate contract for any service or groups of services included in this tendering/RFP.
DIF may negotiate a compensation package and additional provisions to the contract awarded under this tendering/RFP.
DIF reserves the right to debrief the applicants after the completion of the process due to possible high volume of applications and avoiding the compromise of the process.

19.Intellectual Property Rights (IPR) Clause

All intellectual property rights (IPR), including but not limited to copyrights, trademarks, patents, trade secrets, and any other proprietary rights developed, created, or generated under this contract, shall be the exclusive property of HAUS, the project, and the European Union. All communication related to the project will be made in accordance with HAUS.

.2. All intellectual property rights in the Secure Data Infrastructure Management Knowledge Stream package shall be owned by Client upon payment in full to Contractor for the service provision.

The Consultant acknowledges that all deliverables, including but not limited to reports, guidelines, methodologies, databases, training materials, benchmarking tools, and digital repositories, shall be considered "works made for hire" under applicable copyright laws. Consequently, HAUS, the project, and the European Union shall hold full ownership of all such intellectual property developed under this contract.

Any intellectual property pre-existing before the execution of this contract that is incorporated into the deliverables remains the property of the Consultant or its licensors. However, the Consultant grants HAUS a perpetual, irrevocable, royalty-free, non-exclusive, worldwide license to use, reproduce, modify, and distribute such pre-existing intellectual property as part of the deliverables provided under this contract.

The Consultant shall not use, reproduce, license, sell, or distribute any intellectual property developed under this contract for any purpose outside the scope of the agreement without the prior written consent of HAUS. Any commercialization or further development of the work product outside of HAUS' ownership shall require a separate written agreement between the parties.

The Consultant warrants that the deliverables do not infringe upon any third-party intellectual property rights. If any infringement claim arises, the Consultant shall indemnify, defend, and hold HAUS harmless from any liability, damages, costs, or legal expenses resulting from such claims.

The Consultant shall treat all information, data, and materials related to this contract as confidential and shall not disclose or use them for any purpose other than fulfilling its obligations under this contract. Any publication, licensing, or commercial use of HAUS' intellectual property requires prior written approval from HAUS.

The intellectual property rights provisions in this contract shall survive the termination or completion of the contract, ensuring HAUS' continued ownership and use of all developed materials.

D4D HUB

DATA GOVERNANCE IN AFRICA

Global Gateway

Belgium partner in development

Republic of Estonia Ministry of Foreign Affairs

SUOMI FINLAND

german cooperation DEUTSCHE ZUSAMMENARBEIT

Implemented by

Digital Africa · Enabel · estdev From the people of Estonia · Expertise France Groupe AFD · giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH · HAUS

Learn more:

https://d4dhub.eu/initiatives/data-governance-in-africa