NITA UGANDA

- Driving the IT Revolution -

NATIONAL INFORMATION TECHNOLOGY AUTHORITY-UGANDA

TERMS OF REFERENCE

FOR

CONSULTANCY SERVICES TO DEVELOP A CYBER SECURITY STANDARD AND CERTIFICATION FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISES (SMEs)

FEBRUARY 2024

1. INTRODUCTION AND BACKGROUND

NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA (NITA-U), (herein after called "the CLIENT") is an autonomous agency of the Government of Uganda established by the National Information Technology Authority, Uganda Act, 2009 to coordinate, promote and monitor Information Technology (IT) developments in Uganda within the context of National Social and Economic development.

The Government of Uganda, through the National Information Technology Authority, Uganda (NITA-U) has received funding from the World Bank/IDA towards financing the Uganda Digital Acceleration Project – Government Network (UDAP-GovNet). The National Information Technology Authority of Uganda (NITA-U) is the Lead Implementing Agency for this Project. As part of UDAP-GovNet, the goal is to transform the way people, governments, businesses and civil society interact with each other, by supporting digital transactions and e-services that can be delivered in a paperless, cashless and secure manner without the requirement for in-person interaction, which in turn also contributes to climate mitigation. In relation to this, there is an increasing reliance on digital technologies and the growing sophistication of cyber threats have highlighted the critical importance of cybersecurity for small and medium-sized enterprises (SMEs). SMEs play a significant role in driving economic growth and innovation, but they often lack the resources and expertise to effectively address cybersecurity challenges. As a result, they become attractive targets for cybercriminals seeking to exploit vulnerabilities. Traditional cybersecurity frameworks and certification schemes are often designed with larger organizations in mind, making them impractical or too burdensome for SMEs. Recognizing this gap, there is a pressing need to develop customized a cyber security standard (toolkit of prioritized and simplified cybersecurity best practices) and certification framework that cater specifically to the unique needs, resources, and constraints of SMEs.

In order to address the above gap, NITA-U seeks to procure a Firm under contract to develop a customized cybersecurity standard (toolkit of prioritized and simplified cybersecurity best practices) and certification framework for Small and Medium-Sized Enterprises (SMEs).

2. SCOPE OF CONSULTANCY SERVICES

The Consulting Firm shall be required to interact with various players/stakeholders in the Sector including but not limited to associations that represent Small and Medium Enterprises, Private Sector Foundation, Uganda National Bureau of Standards (UNBS), professional bodies and leadership and decision makers from the relevant Ministries and Agencies, and any other relevant stakeholders deemed necessary to provide vital input into the work. National Information Technology Authority – Uganda is the lead agency and coordinator for this assignment.

The assignment will focus on the following:

a) Conduct an in-depth analysis of the cybersecurity challenges faced by SMEs in developing countries, with a focus on African SMEs and those in Uganda in particular - considering their specific industry sectors, size, and resources.
b) Conduct a review of international best practices on cybersecurity standards and certification for SMEs relevant for the African and specifically Ugandan context
c) Develop a customized cybersecurity standard for SMEs in Uganda. The Standards will serve as toolkit of prioritized and simplified cybersecurity best practices for SMEs in Uganda.

d) Develop a certification framework that enables SMEs to undergo assessment and validation against the developed standards

e) Conduct pilot testing of the developed standards (toolkit of prioritized and simplified cybersecurity best practices) and certification framework with a select group of five SMEs to assess their effectiveness and practicality

f) Deliver a two day in person training workshop for a group of no more than 30 Ugandan SMEs. Deliver a two-day face-to-face (in-person) training workshop for a group of no more than 20- auditors / certifiers of Ugandan SMEs

g) Deliver a short, practical note (max 15 pages) re-packaging the findings and recommendations of this research and analysis, with confidential and sensitive information removed, and readied for dissemination in the public domain, so as to contribute to the international body of knowledge on cybersecurity as a global public good.

3.0 KEY DELIVERABLES AND REPORTING

The expected deliverables for this assignment are detailed herein below. The deliverables/outputs Reports shall be submitted in paper (2 hard copies each – signed original and duplicate) and electronic format. The Consulting Firm shall be required to submit electronic reports in MS Word, pdf files (secured) and presentations in MS Power Point. Reports will be submitted in English only.

3.1 Task 1: Inception Stage

Upon signing the contract, the Consultant shall be availed with information and other supporting materials that provide background data (as indicated in section 7 below) to support in the development of the Inception Report. This report will contain full details of the consultant's understanding of the assignment, methodology, project plan, stakeholder engagement plan, project risk management plan, associated resource requirements and timelines subject to NITA-U's approval.

Task 1 Deliverable:
The Consultant shall submit an Inception Report from Task 1.

3.2 Task 2: Conduct Situational Analysis

The Consultant shall undertake a situational analysis of the cybersecurity challenges faced by SMEs in developing countries generally and in Uganda specifically, considering their specific industry sectors, size, and resources. NITA-U will provide the list of the SMEs (not more than 30) for this exercise as well as the necessary introductions. The Consultant shall convene an in-country meeting with NITA-U to review the results of task 2.

Task 2 Deliverable:
The Consultant shall submit the Situational Analysis Report from task 2.

3.3 Task 3: Conduct an international benchmark

The Consultant shall undertake a desk and documentary review of international best practices on cybersecurity standards and certification for SMEs. The consultant shall the list of sources for approval with NITA-U before starting the benchmark. The Consultant shall convene a meeting with NITA-U to review the results of task 3.

Task 3 Deliverable:
The Consultant shall submit the International Benchmark Report from Task 3.

3.4 Task 4: Develop the customized cybersecurity standard (toolkit of prioritized and simplified cybersecurity best practices) for SMEs in Uganda

The Consultant shall develop the customized cybersecurity standard (toolkit of prioritized and simplified cybersecurity best practices) for Ugandan SMEs taking into consideration the findings from the previous tasks above. The focus of the standard should ensure that an SME has the baseline cybersecurity controls in place. Documentation should include a set of practical checklists, toolkits and guidelines to assist SMEs in implementing the cybersecurity standards framework effectively. The standards must be adapted to the characteristics of SMEs and should be adaptable based on the criticality of information processed by the SME, the industry and their dependence on ICT. The toolkit should also include templates for identified policies, procedures and guidelines in simple English that an SME can use to customize to their environment. The Consultant shall also develop educational materials that NITA-U Project Implementation Team will use during engagements with SMEs.. The Consultant shall convene an in-country meeting with NITA-U to review the result of task 4.

Task 4 Deliverable:
The Consultant shall submit the customized cybersecurity standard for SMEs from Task 4.

3.5 Task 5: Develop the certification framework for SMEs

The Consultant shall develop the certification framework for SMEs in Uganda taking into consideration the findings from the previous tasks above. Documentation should outline the comprehensive certification process for SMEs to validate their compliance with the cybersecurity standard. This documentation should include certification criteria, assessment methodologies, application procedures, self-assisted compliance checklists, auditor/certifier process and checklist, requirements and process to accredit an assessor for this standard aligned to the NITA-U certification process (this should also provide a process path for an individual auditor) and recertification guidelines. The Consultant shall propose a workflow to publish the list of certified SMEs on the NITA-U web. The Consultant shall convene an in-country meeting with NITA-U to review the results of task 5.

Task 5 Deliverable:
The Consultant shall submit the certification framework for SMEs from Task 5.

3.6 Task 6: Conduct pilot testing of the developed cybersecurity SME standard (toolkit of prioritized and simplified cybersecurity best practices) and certification framework

The Consultant shall conduct pilot testing of the developed cybersecurity standard (toolkit of prioritized and simplified cybersecurity best practices) and certification framework. NITA-U will provide the list of the five SMEs and five auditors to participate in this process. This process will be a proof of value as well as test both the standards and certification process applicability and validation. The lessons learned and comments collected from the validation exercise will be integrated into the final version of the product. The Consultant shall convene a meeting with NITA-U to review the result of task 6.

Task 6 Deliverable:
The Consultant shall submit the report from the pilot testing of the developed cybersecurity standard and certification framework.

3.7 Task 7: Final Report

The Consultant shall prepare and deliver to the NITA-U a substantive and comprehensive final report and final versions of all deliverables and work performed under these Terms of Reference. It will spell out recommendations to guide NITA-U in implementing the cybersecurity standards for SMEs. The final report should also provide detailed, actionable recommendations to the GoU on any legal amendments, regulatory adjustments, strategy or policy changes and a recommended list of complementary activities to achieve the desired goals of this effort.

Task 7 Deliverable:
The Consultant shall provide a Final Report from this assignment.

Table 1: Deliverables and submission Timelines

No.	**Name of Deliverable**	**Contents of deliverable**	**Timeline for each deliverable**
1	Inception Report	This report will contain full details of the consultant's understanding of the assignment, methodology, project plan, stakeholder engagement plan, project risk management plan, associated resource requirements and timelines	**0.75 months**
2	Situational Analysis report	Provide findings from the situational analysis	**2 months**
3	International Benchmark	Provide findings from the international benchmark	**1 month**
4	Customized cybersecurity standard (toolkit of prioritized and simplified cybersecurity best practices) for SMEs	The Customized cybersecurity standard (toolkit of prioritized and simplified cybersecurity best practices) for SMEs and all related works	**2 months**

No.	Name of Deliverable	Contents of deliverable	Timeline for each deliverable
5	Cybersecurity certification framework for SMEs	The cybersecurity certification framework for SMEs and all related works	**2 months**
6	Cybersecurity standard and certification framework Validation	Cybersecurity standard (toolkit of prioritized and simplified cybersecurity best practices) and certification framework testing and validation results, findings and report	**1.5 months**
7	Final Report	executive summary, the key findings, providing all of the findings, analysis and deliverables	**0.75 months**

4.0 MINUMUM REQUIREMENTS OF THE CONSULTING FIRM AND KEY STAFF

4.1 Requirements for the Consulting Firm

a) Shall be a legally registered organization in Uganda or overseas.

b) The firm must demonstrate previous experience in information security consulting and advisory. The firm should be able to demonstrate their ability to develop and tailor national level cybersecurity standards/ toolkit of prioritized and simplified cybersecurity best practices, cyber security strategies or frameworks to specific target audiences and industries in at least 5 (five) assignments of similar type, scope and nature. Consulting firms should present documentary evidence details of these similar assignments and must include at the minimum signed letters of completion from the clients, scope and proof of certification (including start and finish dates).

c) The consulting firm must demonstrate ability to field a team of experts with required qualifications and experience for the assignment. The team of experts should include local experts due to the heavy workload in-country and nature of assignment (Must present profile for each required expert with mandatory documentation including CV, copies of required certifications and qualifications as well as a section showing the required experience)

d) The consulting firm shall posses a valid ISO 9001 Quality Management Certificate (obtained before publication of this consultancy) to provide assurance that firm has a tested quality approach to their work.

e) Consulting Firms may associate with other firms of a Joint Venture (JV) or a sub consultancy to enhance their qualifications.

The Consulting Firm is required to elaborate in their proposal the envisaged logistical set-up and deployment of appropriate skills for the execution of the assignment. The consultant should carefully review the scope of work and propose a team of well-organized competent staff, adequately equipped with the necessary skills/facilities to execute the assignment, bearing in mind that a substantial amount of work in this assignment is field based in country.

4.2 Expertise and Qualifications of Team Members

The consulting firm should field a team of key experts and non-key experts including among others the following key experts.

4.2.1 Team Leader (1)

Roles and Responsibilities

i. Responsible for the overall management of the assignment and successful timely completion of all deliverables
ii. Ensures the quality of all deliverables by providing guidance and coordinating with team members with their inputs and contribution.

Experience

i. The consultant should have at ten (10) years of experience working on ICT and cybersecurity consultancies, projects with documented experience on leading teams. This must be clearly documented on the CV
ii. Have led at least three (3) projects having similar objectives
iii. The consultant should have a profound theoretical as well as practical knowledge and experience in the relevant fields.
iv. The consultant should have good skills in strategic planning, policy level document development.
v. Excellent written and verbal communication skills.
vi. Excellent planning skills
vii. Fluent oral and written English language skills

Qualifications

i. The consultant should have at least a Bachelor’s degree in Information Technology, Information Security, ICT Management or areas related to this assignment from internationally recognized institution. A copy of this degree award must be provided within the Firm’s proposal.
ii. Certification in any of the following: CISSP/CISA/CISM
iii. Certification in IT service management: ITIL

4.2.2 Cybersecurity Expert (2)

Roles and Responsibilities

i. Responsible for the cybersecurity input for the situational analysis, international benchmark, standards development and certification framework related deliverables
ii. Training SMEs and Auditors on the developed standards
iii. Participating and leading in the validation meetings.

Experience

i. The consultant should have at least five (5) years of experience working on ICT and cybersecurity consultancies, projects with documented experience. This must be clearly documented on the CV
ii. The consultant should have a profound theoretical as well as practical knowledge and experience in cybersecurity
iii. Fluent oral and written English language skills

Qualifications

iv. The consultant should have a Bachelor's degree in Information Technology, Information Security, ICT Management or areas related to this assignment from internationally recognized institution. A copy of this degree award must be provided within the Firm's proposal.
v. The following industry certifications: CISSP/OSCP/CISM and CEH. Copies of these valid certifications must be provided within the Firm's proposal.

4.2.3 ICT Standard/Toolkit Expert (2)

Roles and Responsibilities

i. Responsible for the standards (toolkit of prioritized and simplified cybersecurity best practices) and related drafting input into the development and certification framework related deliverables
ii. Training SMEs and Auditors on the developed standards
iii. Participating and leading in the validation meetings.

Experience

iv. The consultant should have at least five (5) years of experience implementing or auditing cyber security related standards and/ or frameworks as well as working on ICT and cybersecurity consultancies, projects with documented experience. This must be clearly documented on the CV
v. The consultant should have a profound theoretical as well as practical knowledge and experience in cybersecurity
vi. Fluent oral and written English language skills

Qualifications

vi. The consultant should have a Bachelor's degree in Information Technology, ICT Management or related areas from internationally recognized institution. A copy of this degree award must be provided within the Firm's proposal.
vii. The following industry certifications: ISO 27001 Lead Implementor/ SO 27001 Lead Auditor. Copies of these valid certifications must be provided within the Firm's proposal.

4.2.4 Digital Transformation Expert (1)

Roles and Responsibilities

i. Responsible for the digital transformation and related drafting input into the execution of the situational analysis, development of the standard and certification framework related deliverables
ii. Training SMEs and Auditors on the developed standards
iii. Participating and leading in the validation meetings.

Experience

i. The consultant should have at least five (5) years of experience working on ICT related consultancies, projects with documented experience. This must be clearly documented on the CV
ii. Experience in implementing or participating in projects related to digital transformation initiatives for SMEs is desirable (knowledge and expertise of SMEs, their needs, their challenges and how to overcome them)

iii. The consultant should have a profound theoretical as well as practical knowledge and experience in cybersecurity
iv. Fluent oral and written English language skills

Qualifications

i. The consultant should have a Bachelor's degree in Information Technology, ICT Management or areas related to this assignment from internationally recognized institution. A copy of this degree award must be provided within the Firm's proposal.
ii. The following industry certification: ITIL. Copies of these valid certifications must be provided within the Firm's proposal.

5.0 DURATION OF ASSIGNMENT

The assignment is scheduled for a total of ten (10) months from the date of contract effectiveness.

6.0 REPORTING

The selected consulting firm shall report to the Director Information Security or any persons that may be selected by the Director Information Security. In addition, the consultant shall be required to provide a weekly and monthly report detailing progress achieved and/or any difficulties encountered prior to providing the final project report. Further information can be obtained at the address below during office hours from 08:00 to 17:00 hours East African Time (EAT) on working days and from the NITA-U website (http://www.nita.go.ug)

7.0 DATA, SERVICES AND FACILITIES TO BE PROVIDED BY THE CLIENT

The Client will provide the following information, data or reports:

a) National Information Security Framework
b) National Cybersecurity Strategy
c) National ICT Survey Report

8.0 REQUIREMENT FOR QUALITY PLANS

The Consulting Firm will be required to demonstrate in their proposal, evidence of adoption of use of a Quality Assurance System as well as to describe how quality control will be implemented in the course of the assignment.

9.0 PAYMENT SCHEDULE

No.	Description	Percentage
1	After acceptance of the Inception Report	15%
2	Detailed report from the independent situational analysis & International benchmark report	20%
3	Customized cybersecurity standard (toolkit of prioritized and simplified cybersecurity best practices) for SMEs and Cybersecurity certification framework for SMEs	25%
4	Cybersecurity standard and certification framework Validation	35%
5	After acceptance of the Final Report	05%
Total		100%