NITA
UGANDA
- Driving the IT Revolution -

NATIONAL INFORMATION TECHNOLOGY AUTHORITY-UGANDA

TERMS OF REFERENCE

FOR

CONSULTANCY SERVICES TO DEVELOP THE CYBERSECURITY AUDIT AND EVALUATION FRAMEWORK FOR GOVERNMENT OF UGANDA

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. The Government of Uganda (GoU) regards cybersecurity as an enabler of efficient, effective, safe and secure delivery of crucial public services. Cybersecurity also serves broader national security goals by protecting Critical Information Infrastructure. In line with this, GoU developed the National Information Security Framework (NISF) in 2014 to define the minimum information security controls for Ministries, Departments and Agencies (MDAs) across the domains of governance, information security, personnel security and physical security. The focus as per the current National Cybersecurity Strategy is to update the NISF in line with current industry and threat landscape developments as well as create the tools through which Cybersecurity audits and evaluation can be conducted. In addition, the update will also provide the minimum baseline controls for critical information infrastructure as well as Operational Technology.

In order to address the above gap, NITA-U seeks to procure a Firm under contract to develop the cybersecurity audit and evaluation framework for Government of Uganda.

2. SCOPE OF CONSULTANCY SERVICES

The Consulting Firm shall be required to interact with various players/stakeholders in the National Information Security Advisory Group, 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) Review and enhancement of the National Information Security Framework
b) Develop the cybersecurity audit and evaluation toolkit based on item (a) above
c) Develop guidelines for Cyber Threat Modelling
d) Conduct pilot testing of the developed standards and certification framework with a select group of five MDAs to assess their effectiveness and practicality

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: Review and enhance the National Information Security Framework

The Consultant shall undertake a review of the current framework and improve it given the current cybersecurity and threat landscape. In this task, the consultant shall also conduct an international best practices study to identify areas for inclusion and lessons. The enhancement should take into consideration the following:

a) An in-person workshop to obtain feedback from 25 Government entities (these will be selected by NITA-U). This workshop should further seek to obtain MDA input in the effectiveness and usability of the framework.
b) Cybersecurity controls should focus on security outcomes rather than bureaucracy cognizant of the fact that security involves trade-offs
c) Provide for Statement of Applicability where an organization selects the controls applicable to their environment. This will help to an organization achieve the cybersecurity level matching their needs.
d) Requirements for at the minimum Critical Information Infrastructure, Operational Technology, Application Programming Interface and Cloud hosting given its increasing use
e) Detailed guidance notes to assist in implementation so that any entity can self-implement. These notes should simplify the implementation process
f) Maturity levels to guide continuous improvement
g) The resources required by NITA-U to maintain and resources required by MDAs to implement the framework

The Consultant shall convene an in-country meeting with NITA-U to review the result of task 2.

Task 2 Deliverable:
The Consultant shall submit the enhanced National Information Security Framework from task 2.

3.3 Task 3: Cybersecurity audit and evaluation toolkit

Based on the work from Task 2 above, the consulting firm shall proceed to develop the Cybersecurity audit and evaluation framework using widely recognized audit principles, procedures and techniques. This toolkit will be used by both internal and external IT auditors. As such, the toolkit should at the minimum cover the following:

a) Checklists aligned to the enhanced National Information Security Framework
b) Evidence and risk-based auditing
c) Stage based audits for the documentary part and also operations part
d) Creating audit test plans
e) Provisions for conformity and non-conformity
f) Guidance notes for IT auditors and evaluators
g) Guidance notes for effectively reporting audit findings and recommendations to senior management and decision makers.

The Consultant shall convene a meeting with NITA-U to review the result of task 3.

Task 3 Deliverable:
The Consultant shall submit the Cybersecurity audit and evaluation toolkit from Task 3.

3.4 Task 4: Develop the guidelines for Cyber Threat Modelling

The Consultant shall develop the guidelines for Cyber Threat Modelling. These guidelines will assist an implementing organization to comprehensively identify threat events that are relevant to their environment given the increasing use of web services. As such the guidelines must address at the minimum the following areas: technical scoping, system decomposition, threat identification and attack modeling. The guidelines must further include threat modeling scenarios to help facilitate communication by constructing a narrative that can inspire people to act. This is especially important given that decision makers in most organizations do not have IT backgrounds yet they are in charge of allocating resources that the IT and cybersecurity teams would need to address findings from the modelling. The use of scenarios can enhance the remediation effort by helping the IT and cybersecurity teams understand and explain technical matters to business process owners and other stakeholders. Additionally, scenarios help to provide a realistic and practical view of risk that is more aligned with business objectives, historical events and emerging cyber threats forecasted by the organization.

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 guidelines for Cyber Threat Modelling from Task 4.

3.5 Task 5: Pilot testing of the cybersecurity audit and evaluation framework.

The Consultant design and implement in-country the pilot test of the cybersecurity audit and evaluation framework. NITA-U will lead the coordination of five MDAs and ten auditors that will participate in the pilot testing. The results of the pilot should clearly feed back into the design of the audit framework to improve it and make recommendations if needed on capacity building, resource requirements for full scale implementation. As such, the consultant shall use this feedback to update the framework. The Consultant shall lead, guide and facilitate this pilot test. The pilot testing will be conducted in-country. The Consultant shall convene an in-country meeting with NITA-U to review the result of task 5.

Task 5 Deliverable:
The Consultant shall submit the report from pilot testing of the cybersecurity audit and evaluation framework.

3.7 Task 6: Final Report

The Consultant shall prepare and deliver to the NITA-U a substantive and comprehensive final report of all work performed under these Terms of Reference.

Task 6 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	Enhanced National Information Security Framework	All works related to this deliverable	**2 months**
3	Cybersecurity audit and evaluation toolkit	All works related to this deliverable	**2 months**
4	Guidelines for Cyber Threat Modelling	All works related to this deliverable	**1 month**
5	Cybersecurity standard and certification framework Validation	Testing and validation results, findings and report	**1.5 months**
6	Final Report	Executive summary, the key findings, providing all 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 legally registered organizations 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 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) 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 least 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 a Masters'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

ii. 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.
iii. Certification in any of the following: CISSP/CISA/CISM
iv. Project Management certification: Prince 2/PMP

4.2.2 Cybersecurity Expert (2)

Roles and Responsibilities

i. Responsible for the cybersecurity input for tasks 1,3 and 4.
ii. 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

v. 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.
vi. Any of the following industry certifications: CISSP/OSCP/CISM/CEH. Copies of these valid certifications must be provided within the Firm's proposal.

4.2.3 Cybersecurity Auditor (2)

Roles and Responsibilities

i. Responsible for the cybersecurity input for tasks 2 and 4.
ii. 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

vii. 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.
viii. The following industry certifications: CISA and ISO 27001 Lead Auditor. 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 8 months (35 weeks) 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

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.	Enhanced National Information Security Framework	20%
3.	Cybersecurity audit and evaluation toolkit and Guidelines for Cyber Threat Modelling	30%
4.	Cybersecurity standard and certification framework testing and validation results, findings and report	30%
5.	After acceptance of the Final Report	05%
	Total	100%