NITA
UGANDA
- Driving the IT Revolution -

NATIONAL INFORMATION TECHNOLOGY AUTHORITY-UGANDA

TERMS OF REFERENCE

FOR

CONSULTANCY SERVICES TO IMPLEMENT INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) AGAINST THE ISO/IEC 27001 STANDARD FOR TEN (10) PRIORITY INSTITUTIONS

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 the UDAP-GovNet, the project shall focus on strengthening resilience by implementing certified Information Security Management Systems (ISMS) in ten (10) key priority institutions. The priority institutions have been selected based on prior cyber security assessments. In addition, these institutions run critical e-services or hold critical data. Any downtime for from a cybersecurity incident would have a negative business impact on the services offered, data security as well as negatively affect trust amongst citizens. The impact of implementing the ISO 27001 standard in the selected institutions involves reduction of risk of data breaches, trust enablement with citizens but also facilitate compliance with legal requirements (such as the Data Protection and Privacy Act) and fosters a culture of continuous improvement in Government.

This will provide the following benefits to the institutions where this will be implemented:

a) Enhance compliance with the national information security framework requirements.
b) Enhance compliance with legal responsibilities
c) Improve trust in e-service delivery and performance
d) Improve both stakeholder and citizen trust
e) Enhance the institutional cyber resilience
f) Improve internal information security and cyber risk processes and operations based on an international standard
g) Demonstrate Government commitment to taking leadership in implementing a higher maturity of cyber security responsibility and accountability.

In order to establish and implement the above, NITA-U seeks to procure a Firm under contract to design, establish, implement and certify Information Security Management Systems (ISMS) against the ISO/IEC 27001 standard for ten (10) priority institutions including ISO/IEC 27701 and ISO/IEC 20000 for two institutions.

OBJECTIVES

The key objective of the assignment is to carry out a gap assessment, implement any identified remedial works, design, establish, train and implement the ISO/IEC 27001 standard for ten (10) priority institutions including ISO 27701 and ISO 20000 for two institutions and thereafter obtain certification of the same.

SCOPE OF CONSULTANCY SERVICES

The Consulting Firm shall be required to interact with internal stakeholders in NITA-U and project implementation teams from the 10 institutions and any other stakeholders deemed necessary to provide vital input into the work.

The business description for the 10-priority institution is as per the table below:

#	Business Area	Standard	Number of sites	P'le under	Number of certified implementor training	Number of certified auditor training	Organisation HR numbers
Institution 1	Data centre services	ISO 27001:2022	2	15	4	3	120
	IT services (bandwidth provision services)	ISO 20000:2018	2	10	2	2	120
	*Requires self-hosted Governance, Risk and Compliance tool to manage all records related to the standard for 10 users						
Institution 2	Information processing services (on premise)	ISO 27001:2022	1	15	3	2	250
Institution 3	Information processing services (cloud hosted)	ISO 27001:2022 & ISO 27701:2019	1	4	2	2	25
Institution 4	Financial management system (on premise)	ISO 27001:2022	1	15	4	2	500
Institution 5	Information processing system (cloud hosted)	ISO 27001:2022	1	10	3	2	200
Institution 6	Information processing system (on premise)	ISO 27001:2022	1	10	3	2	500
Institution 7	Information processing system (cloud hosted)	ISO 27001:2022 & ISO 27701:2019	1	8	2	2	250
Institution 8	Information processing system (on premise)	ISO 27001:2022	1	8	2	2	230
Institution 9	Information processing system (on premise)	ISO 27001:2022 & ISO 27701:2019	1	8	2	1	180
Institution 10	Information processing system (on premise)	ISO 27001:2022	1	5	2	1	180

The assignment shall be comprised of the following for each of the ten (10) priority institutions:

a) Conduct a gap assessment against the for the as-is operational environment. The assessment should be conducted as per the risk assessment requirements of the ISO 27001 standard. This activity will also include scope affirmation.
b) Implement remedial measures for the mandatory areas related to the required mandatory risk documentation and assessment, policies, procedures, records, definition of measurements/ metrics. This should be done on premise in order to ensure knowledge transfer and participation of the institutional project implementation team
c) Undertake training as per the areas and numbers listed in the above-mentioned table
d) Undertake training for top management of each institution on an executive understanding of the standard and a general education and awareness for all staff. In order to ensure sustenance, the firm should provide a tool (licensed for the certification Lifecyle) that the institution will use for continuous education and awareness training
e) Implement hands on coaching, guidance and reviews to ensure that the appropriate ISMS records are documented and approved over a three-month period. This is to ensure adequacy and sufficiency of records required to pass the certification audit. This phase shall include an internal audit prior to the certification commencement
f) Lead the process of NITA-U obtaining certification as per the listed standard for each institution from an international credible certification body for ISO 27001. The firm will lead identification of the certification body and include all applicable fees for the certification audit, first and second surveillance audits
g) Transfer of Knowledge - In order to promote skills development, lesson learning and knowledge sharing, the consultant will submit a knowledge transfer plan to be embedded in the proposal. The Consultant will at the conclusion of the assignment submit as a section in the completion report, achievements made in the Transfer of Knowledge.

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 such as CDROM or Universal Serial Bus (USB) devices. 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.

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 8 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. The Inception Report should include a Knowledge Transfer plan to facilitate skills development and knowledge sharing.

Task 1 Deliverable:

The Consultant shall submit an **Inception Report** from Task 1.

Task 2: Conduct the ISMS Gap Assessment

The Consultant shall undertake a gap analysis of the as-is operational environment of the listed institutions. This should be conducted as per the risk assessment requirements of the ISO/IEC 27001, 20000 and 27701 standards. The gap assessment report should include the results/ findings from the risk assessment, areas of non-conformity, a section on risk treatment, required resources, implementation roadmap and the Statement of Applicability. The Consultant shall convene a meeting with each institution's project implementation team prior to NITA-U approval.

Task 2 Deliverable

The Consultant shall submit the **Gap Assessment Report, include the Remediation Plan** as well as the Statement of Applicability for each institution.

Task 3: Conduct Capacity Building

The Consultant shall carry out capacity building as noted below:

a) Executive training for top management of each institution on understanding of the standard. This will take place in each institution's boardroom

b) General education and awareness for all staff. In order to ensure sustenance, the firm should provide a cloud-based awareness tool (licensed for the certification Lifecyle) that the institution will use for continuous education and awareness training. As such, the firm should have vendor authorization for the supplied tool. The vendor must include this requirement in the methodology and pricing. Each of the ten institutions will have their own tool (following numbers in the table above).

c) Professional certified training for implementors and auditors as per the numbers provided for each institution. The firm should include all costs (including venue, catering, full board accommodation and related logistics) applicable to the professional training material, exam and five-day bootcamp fully covered in a venue in Kampala, Uganda. In addition, the firm shall provide six copies of the ISO 27001 standard (latest versions) to each of the ten institutions and three copies of the ISO 20000 and ISO 27701 for two institutions.

Task 3 Deliverable

The consultant shall provide material in form of material, presentations and text useful in the implementation of the standards as stated above. In addition, the Consultant shall submit a **Capacity Building report** for each institution.

Task 4: ISMS Records implementation

The firm shall implement hands on coaching, guidance and reviews to ensure that each institution is creating the appropriate ISMS, SMS and PIMS records and that they are documented and approved. This will be done over a three-month period. As such, the firm needs to factor in the cost of having the implementing team on premise during the implementation period. This is to ensure adequacy and sufficiency of records required to pass the certification audit. At the conclusion of the three-month period, the firms shall take lead in an internal audit collaborating with the internal audit team or appointed internal Implementation teams to meet standard requirements prior to the certification commencement. In addition, the firm shall supply and set up (and train users) an on-premise/ self-hosted Governance, Risk and Compliance tool with three-year licensing for institution one (10 users). As such, the firm should have vendor authorization for the supplied tool. The vendor must include this in their pricing and methodology. All these will be done on premise to ensure the respective management systems' implementation and records of evidence meet the standards requirements. The implementation arrangement for this deliverable requires on premise in country presence for smooth execution as it's a key phase of the project. Firms should have a local partner or plan accordingly for the on-premise in country presence requirement for this task.

Task 4 Deliverable
The Consultant shall provide a report showing all works done to for the hands-on technical support, the internal audit report and readiness brief for certification.

Task 5: Certification
The Consultant shall lead the process of each institution obtaining certification as per the listed standard for each institution from an international credible certification body for ISO 27001, ISO 20000 and ISO 27701. The consultant is required to identify and engage a reputable certification body and include all applicable fees for the certification audit, first and second surveillance audits.

Task 6 Deliverable
The Consultant shall submit a report showing certificate report, the certificate for each institution and attendant documentation.

Table 1: Deliverables and submission Timelines

No.	Name of Deliverable	Contents of Deliverable	Time for each phase
		Assessment Phase One	
1.	Inception Report	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	4 weeks
2.	ISMS Gap Assessment	Gap Assessment Report, include the Remediation Plan as well as the Statement of	8 weeks

		Applicability for each institution.	
3.	Capacity Building	Includes the results/ findings from the executive training, implementor certified training, auditor certified training, staff education, awareness tool licensed for a three-year period	4 weeks
4.	ISMS, SMS and PIMS Implementation	Report showing all works done to for the hands-on technical support, the internal audit report and readiness brief for certification.	13 weeks
5.	Certification	report showing certificate report, the certificate for each institution and attendant documentation.	6 weeks
6.	Final Report	executive summary, the key findings, providing all of the findings, analysis and deliverables and an aggregation of all Tasks including a consultancy completion report, and the recommendations for further development of project	4 weeks

The assignment is scheduled for a total of thirty-nine (39) weeks from the date of contract effectiveness.

MINUMUM REQUIREMENTS OF THE CONSULTING FIRM AND KEY STAFF

Requirements for the Consulting Firm

a) Shall be legally registered organizations in Uganda or overseas

b) The firm must demonstrate previous continuous experience and expertise in handling Information Security Management System and ISO 27001 implementations in at least 5 (five) assignments of similar type, scope and nature within the last 6 (six) years. All the supported clients should have achieved ISO 27001 Certification. The list of previous experience should include at least two data centers. 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 consultants must demonstrate ability to field a team of experts with required qualifications and experience for the 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). The implementation part requires on premise in-country presence for smooth execution. Firms should have a local partner or plan for this.

d) The firm must have valid and current ISO 27001 certification. Additional ISO 27701 and ISO 20000 certification of the firm will be of an advantage. These must have been obtained before the date of publication of this ToR. This provides us assurance the consulting firm has itself implemented, achieved certification and maintained the ISMS as per ISO 27001, 20000 and 27701 standards

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

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.

Team Leader (1)

Roles and Responsibilities

a) Responsible for the overall management of the Project and successful timely completion of all deliverables
b) Ensures the quality of all deliverables by providing guidance and coordinating team members with their inputs and contribution

Experience

a) The consultant should have at least ten (10) years of experience in information security consulting as well as IS auditing with demonstrable experience on the ISO 27001
b) Have led at least five (05) projects having similar objectives;
c) The consultant should have good skills in strategic planning, policy level document development and general information security consulting
d) Fluent oral and written English language skills

*The CV must clearly show the areas indicated above.

Qualifications

a) The consultant should have a Bachelor's Degree in Information Technology, Telecommunications, Information Systems, Business, Computing, Statistics or related areas from internationally recognized institution.
b) Should have both the valid ISO 27001 Lead Audit and ISO 27001 Lead Implementer professional certification
c) Certification in the Project Management field is required
d) Certification in a data privacy related area is required

*The CV must have the attachment to show documentary for each of the qualifications above.

ISMS Audit Lead (1)

Roles and Responsibilities

a) Plan and lead Gap Analysis against the ISO 27001
b) Plan and lead ISMS Internal Audit
c) Plan and lead Risk Assessments and suggest mitigation plans

Experience

a) The consultant should have at least five (5) years of experience in information security consulting and IS auditing with demonstrable experience on the ISO 27001
b) Have led at least five (5) projects having similar objectives;
c) Fluent oral and written English language skills

*The CV must have the attachment to show documentary for each of the qualifications above.

Qualifications

a) Should have a Bachelor's degree in Information Technology, Telecommunications, Information Systems, Business, Computing, Statistics or related area from a recognized university
b) Should have the valid ISO 27001 Senior Lead Auditor professional certification
c) Should have valid data privacy certification

*The CV must have the attachment to show documentary for each of the qualifications above.

ISMS Auditor (2)

Roles and Responsibilities

a) Conduct Gap Analysis against the ISO 27001
b) Conduct ISMS Internal Audit
c) Conduct Risk Assessments and suggest mitigation plans

Experience

a) The consultant should have at least five (5) years of experience in information security consulting and IS auditing with demonstrable experience on the ISO 27001:2013. CV must clearly show this experience.
b) Have led at least three (3) projects having similar objectives; CV must clearly show this requirement
c) Fluent oral and written English language skills

*The CV must have the attachment to show documentary for each of the qualifications above.

Qualifications

a) Should have a bachelor's degree in information technology, Telecommunications, Information Systems, Business, Computing, Statistics or related area from a recognized university
b) Should have the valid ISO 27001 Lead Auditor professional

*The CV must have the attachment to show documentary for each of the qualifications above.

ISMS Implementer (4)

Roles and Responsibilities

a) Conduct ISMS implementation
b) Development of ISMS required documentation and templates
c) Provide hands on technical support and coaching for all ISMS implementation related activities

Experience

a) The consultant should have at least five (5) years of experience in ISMS implementation and information security consulting with demonstrable experience on the ISO 27001 standard
b) Have participated in at least three (3) projects having similar objectives; CV must clearly show this requirement
c) Fluent oral and written English language skills

*The CV must have the attachment to show documentary for each of the qualifications above.

Qualifications

a) Should have a bachelor’s degree in information technology, Telecommunications, Information Systems, Business, Computing, Statistics or related area from a recognized university
b) Should have the valid ISO 27001 Implementation related professional certification

*The CV must have the attachment to show documentary for each of the qualifications above.

SMS Implementer (1)

Roles and Responsibilities

d) Conduct SMS implementation
e) Development of SMS required documentation and templates
f) Provide hands on technical support and coaching for all SMS implementation related activities

Experience

d) The consultant should have at least five (5) years of experience in SMS implementation and information security consulting with demonstrable experience on the ISO 20000 standard
e) Have participated in at least three (3) projects having similar objectives; CV must clearly show this requirement
f) Fluent oral and written English language skills

*The CV must have the attachment to show documentary for each of the qualifications above.

Qualifications

c) Should have a bachelor’s degree in information technology, Telecommunications, Information Systems, Business, Computing, Statistics or related area from a recognized university
d) Should have the valid ISO 20000 Implementation related professional certification

*The CV must have the attachment to show documentary for each of the qualifications above.

Information Security Specialist (1)

Roles and Responsibilities

a) Conducting information security assessments
b) Assist with the development of the mitigation plans

Experience

a) The consultant should have at least three (3) years of experience in information security consulting and IS auditing
b) Have led at least two (2) projects having similar objectives;
c) Fluent oral and written English language skills

*The CV must have the attachment to show documentary for each of the qualifications above.

Qualifications

a) Should have a Bachelor's degree in Information Technology, Telecommunications, Information Systems, Business, Computing, Statistics or related area from a recognized university
b) Should at least one of the following professional certifications or related ones: CISSP, Lead Penetration Tester, CEH, CISM, OSCP, eJPT

*The CV must have the attachment to show documentary for each of the qualifications above.

Data Center Specialist (1)

Roles and Responsibilities

a) Provide IT audit technical assistance to the team
b) Assist with the development of the mitigation plans
c) Train stakeholders
d) Conduct/ assist in vulnerability assessment and in closure of vulnerabilities

Experience

a) The consultant should have at least three (3) years of experience in the deployment and maintenance of a busy virtualized environment
b) Have led at least two (2) projects having similar objectives;
c) Excellent analytic written and verbal communication skills
d) Excellent planning skills
e) Fluent oral and written English language skills

*The CV must clearly show the areas indicated above.

Qualifications

a) Should have a Bachelor's degree in Information Technology, Telecommunications, Information Systems or related area from a recognized university
b) Should have training in administration and support of VMware, Windows Clusters and converged infrastructure.

*The CV must have the attachment to show documentary for each of the qualifications above.

Personal Data Privacy Specialist (1)

Roles and Responsibilities

a) Provide technical assistance to the team and guide implementation of personally identifiable data
b) Assist with the development of mitigation plans
c) Assist with the development of required policies, procedures, template, KPI and measurement metrics
d) Conduct and assist in documentation of privacy assessments
e) Train participants in personal data protection and privacy implementation

Experience

a) The consultant should have at least two (2) years of experience in training and implementation of personal data protection and privacy related frameworks/ standards.
b) Have led at least two (2) projects having similar objectives;
c) Fluent oral and written English language skills

*The CV must have the attachment to show documentary for each of the qualifications above.

Qualifications

c) Should have a Bachelor’s degree in Information Technology, Law, Telecommunications, Information Systems, Information Security, Business, Computing or related area from a recognized university
d) Should have at least one of the following professional certifications: CDPO, ISO 27701 Implementer, CDPSE, CIPM, CIPT or CIPP/E.

*The CV must have the attachment to show documentary for each of the qualifications above.

ISO 27001 Audit Trainer (1)

Roles and Responsibilities

a) Conduct the executive training
b) Conduct the ISMS Audit training

Experience

a) The consultant should have at least two (2) years of experience in training ISMS ISO 27001 Audit
b) Fluent oral and written English language skills

*The CV must have the attachment to show documentary for each of the qualifications above.

Qualifications

a) Should have a Bachelor's degree in Information Technology, Law, Telecommunications, Information Systems, Information Security, Business, Computing or related area from a recognized university
b) Should have at least one valid ISO 27001 Audit professional certification
c) Should have certificate issued by a credible certification body showing authorisation to train ISO 27001

*The CV must have the attachment to show documentary for the qualifications above.

ISO 27001 Implementer Trainer (1)

Roles and Responsibilities

c) Conduct the executive training
d) Conduct the ISMS Implementor training

Experience

c) The consultant should have at least two (2) years of experience in training ISMS ISO 27001 Implementation
d) Fluent oral and written English language skills

*The CV must clearly show the areas indicated above.

Qualifications

d) Should have a Bachelor's degree in Information Technology, Law, Telecommunications, Information Systems, Information Security, Business, Computing or related area from a recognized university
e) Should have at least one valid ISO 27001 Implementor professional certification
f) Should have certificate issued by a credible certification body showing authorisation to train ISO 27001

*The CV must have the attachment to show documentary for the qualifications above.

ISO 27701 PIMS Trainer (1)

Roles and Responsibilities

e) Conduct the executive training
f) Conduct the ISMS PIMS training

Experience

e) The consultant should have at least two (2) years of experience in training ISO PIMS
f) Fluent oral and written English language skills

*The CV must clearly show the areas indicated above.

Qualifications

g) Should have a Bachelor's degree in Information Technology, Law, Telecommunications, Information Systems, Information Security, Business, Computing or related area from a recognized university
h) Should have at least one valid ISO 27701 Audit or implementor professional certification
i) Should have certificate issued by a credible certification body showing authorisation to train ISO 27701 PIMS

*The CV must have the attachment to show documentary for the qualifications above.

DURATION OF ASSIGNMENT

The assignment is scheduled for a total of thirty-nine (39) weeks from the date of contract effectiveness.

REPORTING

The selected consultant 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)

DATA, SERVICES AND FACILITIES TO BE PROVIDED BY THE CLIENT

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

a) ISMS related documentation for each institution
b) National Information Security Framework

REQUIREMENT FOR QUALITY PLANS

The Consultant 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 project.