Republic of South Sudan

South Sudan Revenue Authority(SSRA)
Terms of Reference for Development of the NRA ICT Strategy and Policy Framework

I. Position Information:

1.	Description of Assignment:	Consultancy Services for Development of the NRA ICT Strategy and Policy Framework
2.	Consultancy Type	Consultancy Firm
3.	Project Names	Non-Oil Revenue Mobilisation and Accountability in South Sudan (NORMA) Project
4.	Duration of Assignment	Three (3) months
5.	Duty station	Juba
6.	Starting date	January 2024
7.	Host Agency/Host Institution	South Sudan Revenue Authority(SSRA)

II. Background and Context of the Assignment:

NRA ICT initiatives currently operate at a maturity level below 1. Key products have been inherited from NRA antecedents. There is no formal strategic or tactical planning framework. Application software has also been developed as 'fit around' modifications to imported products without studying and agreeing requirements. ICT processes rely on the opinions driven by the skills of a few people without an ICT policy framework.

Box 1 provides a snapshot of selected aspects considered by NRA to critical in the proposed strategy and policy framework.

Box 1. Remarks arising during research for these TOR

Domestic taxes administration

The Strategy should highlight and cater for:
- sustainability and preferably ownership of NRA ICT assets
- scalability of ICT solutions
- application software products that are readily configurable (and readily customizable where necessary) preferably with in-house resources
- requirements and design developed through consultation with affected user areas
- the deployment and operation of ICT assets determined by NRA policies and requirements rather than set to suit external agenda
- effective interconnection of NRA offices
- interoperation among NRA systems and with external systems
- automation of operations using modern ICT in line with international, good practice for tax administration
- the need for modernized standard operating procedures enabled by and aligned to modern ICT solutions using workflow / business process orchestration

Furthermore, the Strategy should
- provide a practical roadmap for retiring the DTIS, avoiding running parallel systems
- review the progress against the NRA- Crawford e-Tax roadmap and make recommendations appropriately
- review the operations of non-tax revenue and recommend how such functionality can be accommodate in e-Tax
- review the integration requirements for Domestic Taxes and embed them in the overall systems architecture
- review the "to be" processes for Domestic Taxes and recommend any other automation mechanisms for Domestic Taxes
- propose solutions to be used by the Domestic Taxes to automate taxation of entities such as hotels, properties, or warehouses
- review and recommend mechanisms of delivering services closer to taxpayers bearing in mind the poor internet connectivity and poor power supply

Customs administration
- The current system being used by Customs called e-customs seem short of basic standards of a customs systems. It is currently being operated in two ports: Nimule and Juba International Airport. Customs has more than 8 official border sstations requiring automation.
- The Strategy should
  - assess infrastructure, equipment, and software needs for the commercial border points
  - assess the adequacy of e-customs system and suggest possible interventions to

---

2

    enable normal automated operations of the customs environment
- o review and recommend the possibility of activating the WCO membership to enable NRA to benefit from WCO wide ranging support
- o review the licensing regime for clearing agents and propose a mechanism to automate licensing of clearing agents
- o review the conceptual configuration of the regional electronic cargo tracking system and recommend how NRA can participate
- o review and recommend data sharing mechanisms for Customs and other third-party entities

Corporate Planning
- It is important for NRA to have
  - o functioning quality management approach to its ICT (and other) products. The QM approach would include quality assurance independent of the service provider or service developer
  - o appropriate and adequate in-house skills and responsibilities for its operations through continual training programs and policies that increase retention of trained personnel
- The eventual e-Services product should be such that it
  - o ensures effective, efficient, and secure systems for NRA
  - o has modern architectures for effective, secure interoperation (data and message flows) within the systems of NRA (such as between tax and customs for credibility and consistency cross-checks) and with external agencies (for operational effectiveness such as between the banking system and NRA systems, and for credibility and consistency cross-checks)
- The ICT Strategy should
  - o include recommendations for the operationalization of the strategy
  - o be practically achievable – cognizant of the financial capacity for implementation and sustainability
  - o highlight the need for the legality of operation (e.g., through law and regulation for e-transactions, data protection, and data access rights to other agencies by NRA)

Internal Audit
 The Strategy should
- recommend tools for automating Information Systems audits
- review the possibility of the Internal Audit depart to be accredited to Information Systems Audit and Control Association (ISACA) for possible assistance with systems audit techniques

Internal Affairs
 The Strategy should assess the business processes for the internal affairs department and recommend tools to be used to monitor staff integrity issues

Economic Intelligence

 The Strategy should review and recommend data sources or interface requirements to enable automated information gathering for purposes of economic intelligence

Legal Administration
 The Strategy should
- highlight the need for the legality of the operation and indicate the approach to ensuring this

	• include legal opinion during quality assurance of any system design	

III. Current ICT Assess – application software:

Application software assets for tax administration comprise a legacy Domestic Taxes Information System (DTIS) that is being retired and replaced by a new e-Tax application.

DTIS has an application architecture unsuitable for a modern web-based, multi-user service and has an unsafe support basis with the provider no longer able to provide the necessary services.

The new e-Tax application has few elements of a basic functional core for tax administration, limited to recording details for creating and payment obligation and then reconciling the receipt of payment through the banking system and an external, central, privately-held deposit account. The limited functions available are reported to have operational defects. The e-Tax needs significant repair and enhancement to be the asset that NRA aspires to have, and to be in line with international platforms. At the time of writing retirement of the DTIS is stalled due to e-Tax deficiencies such as handling of arrears (for which the records are only in DTIS).

There is no legacy ICT support for Customs administration. An e-Customs product is also evolving, however, again the current e-Customs module is severely deficient functionally, e.g. in comparison to the readily-available Asycuda World product and program available for UNDP / UNCTAD. The trial product again has few elements of a basic functional core for customs administration, limited to recording details for creating and payment obligation and then reconciling the receipt of payment through the banking system and an external, central, privately-held deposit account. The limited functions available are reported to have operational defects.

Together e-Tax and e-Customs are referred to as NRA e-Services under a wider government service provision contract. These services are developed, supported, and hosted in private facilities in Nairobi. There are plans for NRA to assume responsibility for ownership of e-Services in the near-term, however, there are practical impediments relating to readiness in terms of product scope and reliability and NRA skills sets that challenge the efficacy of these plans.

NRA also is in the process of using a Ministry of Finance Integrated Financial Management Information System (IFMIS) (which uses the FreeBalance Application Suite) for expenditure records management.

The NRA Strategy 2022-27 indicates an intention to acquire Human Resource Management Information System (HRMIS), software for management of electronic cargo seals, and other office automation software normally found in modern revenue administrations.

Current ICT Assets – technical infrastructure[1]:

NRA technical infrastructure remains inadequate in several aspects, however, there are plans for improving the conditions.

DTIS is a Microsoft Access desktop application for which NRA has source code. E-Services are currently hosted in Kenya.

Plans are in place for having NRA technical infrastructure for e-Services hosted in a new government data center in Juba. NRA has plans and AfDB financial support for its own data center in Juba that will become the primary NRA data center, prospectively within 12 months from the time of writing. NRA assets in government data center will take on the role of a back-up site.

Juba offices are reported to have usable end-user devices and internet-connectivity. The current connectivity is reported to be quite expensive (reported to be around USD900,000 p.a.) and usage of wider government provided network connections is expected in due course. The customs office / one-stop border post in Nimule (Uganda

---

[1] Technical infrastructure in this context means ICT equipment, appliances, system software, and services at data centers, in telecommunications networks, and at end-user locations.

border) is reported to also have usable set of end-user devices and internet connectivity. Other offices at borders and in NRA state offices are reported to have few or no ICT resources. A program is under-way for VSAT[2]-based carrier services for NRA offices is work-in-progress with AfDB support.

<u>National ICT environment</u>

National ICT technology/infrastructure in South Sudan is also at a low state of development. In particular, this indicates that NRA will need to consider various approaches for office interconnections – as indicated above regarding VSAT-based services.

Programs are planned for national improvements in ICT. A draft Digital Government Strategy has been prepared and may be made available to the selected Consultant. In addition to several good-practice guidelines and recommendations concerning lifting national ICT-literacy and access, the national program includes specific plans that may benefit NRA, namely, (1) ensuring a sound legislative / regulatory framework for electronic transactions, (2) development of a government data center, and (3) development of modern national telecommunication services, suitable for high-availability, high bandwidth data communications.

IV. Required ICT Strategy and Policy Framework:

NRA seeks to develop its first formal ICT Strategy and Policy Framework and seeks to develop this with the assistance of a qualified and experienced Consultant.
The ICT Strategy need to align with the NRA Strategic Plan, contributing to NRA's modernization objectives.
The ICT Strategy and Policies need to be aligned with the NRA business strategy and npriorities.
The ICT Strategy and Policies should be guided by national ICT strategy and policy.
The Objectives in the NRA Strategic Plan present opportunities and demands for enabling ICT environments, tools, processes, and products. The following objectives are particularly relevant to the ICT Strategy and Policies:

1. Leveraging on ICT to transform NRA processes
   [including plans for modernized ICT infrastructure for primary and disaster recovery sites and for the offices network at states and borders, HRMIS, and internal support systems for finance, procurement, internal audit, research, planning, revenue accounting]

2. Enhance voluntary compliance
   [including plans for an integrated tax administration software system comprehensively covering modernized tax administration business processes, and electronic fiscal devices]

3. Enhance trade facilitation
   [including plans for an integrated cross-border management system, automated customs system, electronic cargo tracking, a risk management system, and potentially a trade single window]

4. Strengthening customer service
   [including plans for effective and efficient taxpayer service channels, and taxpayer feedback mechanisms]

5. Enable systems, data and processes integration across all NRA activities

6. Improve data quality, analysis, reporting and decisions making
   [including plans for an Enterprise Data Warehouse and a business intelligence and data analytics capability]

7. Enable remote online access to systems from anywhere, anytime and any device.

---

[2] VSAT means Very Small Aperture Terminal for satellite-based telecommunications.

8. Ensure strong security of systems and data

V. Objectives of the Assignment:

NRA, South Sudan desires to have an ICT Strategy and Policy Framework tailored for its needs covering the whole of NRA. This effort must

(1) assess the current ICT conditions for all operating units and locations of NRA,

(2) Assess the level of ICT infrastructure in the country,

(3) Undertake a benchmark analysis of national revenues authorities' ICT strategies and policies at the regional level in at least 3 countries (to be determined) which have the most advanced NRA ICT infrastructures,

(4) Define the future ICT infratucture needs of NRA and provide a gap analysis, and

(5) Develop a four-year strategy (aligned to the current corporate strategy timeline) that provides short-term, medium-term and long-term guidance for NRA's ICT needs.

The ICT Strategy and Policy should be aligned to the NRA Strategic plan 2022 – 2027. The development of the ICT Strategy and Policy will be preceded by an operational review of the current ICT department, application software, data center, end-user site equipment, and network infrastructure. The goal is to ensure that business technology services are a platform for innovative and progressive business process improvements that will assist in ensuring the effective and efficient delivery of high-quality services by NRA's departments to the Taxpayers and to those that do business with NRA.

The assignment will require in-country activities for research and presentations, at a minimum, and may also include activities done remotely, including, additional research, presentations, progress meetings, analyses, and report-writing. The adequacy of the proposed approach will be akey in the assessment of any proposal for this assignment.

VI. Scope of the work:

Part 0: Inception

Within the first five business days of the start of the assignment, the Consultant is required to investigate extant conditions related to the assignment and develop and present an Inception Report to the NRA Management. The Inception Report will document inception stage findings and update the work plan that the Consultant provided at proposal submission. The Consultant shall proceed with the assignment after acceptance of the Inception Report by NRA Management .

Part 1: ICT Strategy

The Consultant will conduct an assessment and provide recommendations to address immediate, short- medium- and long-term corporate strategies, opportunities, vulnerabilities and needs.

The ICT Strategy shall be aligned with the NRA Strategic Plan and lay out the path to actualizing the Strategy and vision across NRA and particularly in ICT, given the resources identified in the assessment phase of the assignment. The Consultant is expected to collaborate continuously with NRA staff and external institutions in the whole process of Strategy development and shall update NRA Management regularly on progress through weekly reports and through meetings as may be necessary.

It is expected that the Consultant will then facilitate a participatory process to review arising recommendations and determine the future direction of ICT at NRA.

Part 2: Initiatives, Projects, and Profiles

As described above, the Strategy must define the portfolio of projects and internal initiatives that would take NRA from its existing condition and architecture to the desired condition and architecture. The projects and initiatives shall be prioritized and sequenced.

When the ICT Strategy is broadly accepted by NRA,

1. Define for each project, a project profile encompassing:

   ▪ Project objective

   ▪ Project principal target products and sub-products and high-level attributes of each product

   ▪ High-level tasks descriptions and sequencing

   ▪ Estimated timeline

   ▪ Project organization: project owner, project manager, team roles and staffing number estimates, with skills and experience profiles, and expected engagement with persons external to the project

   ▪ Resource estimates – human resource, financial, and other resources, both internal and external contributors of the needed resources

   ▪ Relationship to other projects in the portfolio and to initiatives

   ▪ Dependencies

   ▪ Other notes as may arise

     For each initiative, define:

   ▪ Objective

   ▪ Target outcomes

   ▪ Tasks

   ▪ Resourcing

   ▪ Relationships to other initiatives and projects

   ▪ Dependencies

   ▪ Other notes as may arise

2. Consolidate an overall estimated Strategy financial requirement covering recurrent costs for operations, costs of initiatives, and project costs and present the estimated financial requirement over a four-year timeline.

3. Present the project profiles to the NRA Management and review as necessary.

Part 3: ICT Policies

The Bidder shall demonstrate how it proposes to obtain and assess vulnerabilities and gaps in existing formal and informal ICT Policies of NRA and how it proposes to collaborate with NRA ICT team and other parties as may be required to expand and update the existing policies. The expanded and updated ICT Policies shall cover at least the topics described below.

Introduction – ICT Policies requirements

Information and Communication Technology (ICT) describes various technologies that make information and communication services available to a wide range of users. The term is used broadly to address a range of established and relatively new technologies, among which include:

- *Information Technology (IT)* which uses computers that have become indispensable in many organizations to process any volume of data and save time and effort.

- *Telecommunications technologies* which include telephones (with fax) and the broadcasting of audio and visual data, usually through high-speed media such as fiber optic or satellite.

- *Networking technologies* and unified communications which include the Internet, mobile phone technology, Voice Over IP telephony (VOIP), and satellite communications.

Securing information has become increasingly complicated in the current era, especially in a complicated environment such as a Revenue Authority. Security threats are a major concern in such an environment. Threats come in different forms, ranging from physical to logical threats. These can again be subdivided into various types of threats, and they all need to be managed. Such threats originate from outside and also from within the NRA domain; they may be on the Network, Servers, Desktops or Laptops and may affect operations in different ways.

The commonly known ways in which these threats affect operations is by compromising confidentiality, integrity, and availability through means such as:

- denial of service

- interception of information

- modification of information.

Objectives – ICT Policies requirements

The ICT Policies are expected to provide a regulatory framework in which ICT is operationalized and managed in a standardized way. The ICT policies are also aimed at addressing the current and future potential threats and vulnerabilities to information and data stored on NRA devices such as servers, computers, or mobile gadgets. Information and data must be secured in a way that ensures its integrity, availability, and confidentiality.

In summary, the ICT Policies are expected to have three objectives:

- protect all NRA ICT infrastructures and information from unauthorized access and disclosure

- ensure that the information is available in an unaltered form at all times

- provide management direction and support for ICT.

Scope – ICT Policies requirements

The required policies should accordingly apply to:

- All NRA departments, employees, contractors, and consultants:

  - having access to and/or using NRA's ICT resources

- o administering NRA's ICT resources

- o storing any non-public NRA information

- o dealing with requisition, procurement, replacement and upgrading of NRA ICT resources such as computer hardware, accessories, and software.

- All NRA ICT resources currently in existence and to any new automation technology that will be acquired in future, at all levels of sensitivity, whether maintained in-house or commercially. These ICT resources include, but not limited to:

  - o application software, both outsourced and in-house developed applications

  - o system software, e.g., Windows Operating System and Linux

  - o computer equipment and all related hardware, whether it is network equipment or standalone workstations

  - o communication systems and equipment, e.g., telephones and radios

  - o networking systems and equipment, e.g., switches and cables.

  Reference to this document shall also be made in all contracts with external entities.

Remedies for breaches – ICT Policies requirements

Punishment for violating any one of the policies contained in this document shall be given, depending on the type of offence and offender, e.g.:

- Staff: Punishment shall be in accordance with NRA's Disciplinary Procedure Code

- Contractors and consultants: Violation shall be a breach of the engagement contract

- Non-IRD Staff: Disabled from using NRA ICT facilities and follow appropriate legal provisions.

- External Users (Taxpayers and other stakeholders): Disabled from using NRA ICT facilities for a specified period and follow appropriate legal provisions.

- Students: Applicable measures shall be taken which may include termination of attachment (internship, research, etc.).

All in all, the Consultant is expected to develop ICT Policies that include but not limited to these listed below.

Item	Policy area	Sub policies
1	ICT HARDWARE AND OTHER EQUIPMENT	
		• Acquisition policy • Installing new hardware policy communication systems policy • Computer networks policy • Computer systems operation and administration policy • Disposing of obsolete equipment policy • Hardware insurance policy • Equipment relocation policy
2	ACCESS CONTROL	
		• Access account and password policy • Logon and logoff policy • Clear screen policy • Access rights control policy
3	CONTROLLING INFORMATION	
		• Policies update policy

- Procedures and standards update policy
- Confidentiality agreements policy
- Internet access policy
- Email policy
- Facebook policy
- Backup, recovery and archiving policy
- Personal computer policy
- ICT governance framework policy

4   APPLICATION SYSTEMS
- Software development and acquisition policy
- System enhancement policy
- Implementing new/upgraded software policy
- Application support policy
- Application platform policy
- Illegal applications policy
- Business continuity policy
- Incident management policy
- User and administrator training policy
- Documenting systems policy
- Software amendments policy
- Disposal of software policy
- Managing program source libraries policy
- User acceptance policy
- Project methodology policy

5   PHYSICAL AND ENVIRONMENTAL SECURITY
- Physical security
- Physical access controls
- Protection against environmental threats

6   LOGICAL SECURITY
- User accounts and passwords

7   NETWORK SECURITY
- Physical network security
- Logical network security
- Access control lists
- Intrusion detection and prevention
- Intrusion prevention and security monitoring

8   INTERNET/INTRANET/EXTRANET SECURITY
- Internet
- Intranet
- Extranet security

9   ANTI VIRUS SECURITY
- Anti-virus
- Scan for vulnerabilities

10   VENDOR SUPPORT
- Logs
- Log reviews

11   INFORMATION SECURITY
- Information ownership
- Data protection
- Securing electronic transactions
- Data leak prevention

12   BACKUPS

- Configuration backup
- Systems backup
- Data backup

13   HELPDESK/SERVICE DESK INCIDENT MANAGEMENT POLICIES

VII. Team Composition & Qualification Requirements for the Key Expert:

NRA requires a Consultant with diverse skills set and proven experiences that would not reside in a single individual. The skills set and experiences needs to cover:

1   Domestic Tax and Customs administration systems

2   Internal administration systems as part of running the business of a national revenue administration

3   In-depth practitioner knowledge of application software for integrated tax administration

4   In-depth practitioner knowledge of application software for integrated customs administration

5   ICT strategy formulation for public sector revenue administration, across domestic taxes and Customs, and internal non-core processes of a national revenue administration

6   ICT strategy formulation for the various aspects of technical infrastructure (data center ICT, telecommunications ICT, cyber-security) for a public sector organization of national significance and scope.

7   Formulation of ICT Policies for a public sector organization of national significance and scope.

Taken together, the Bidder's proposed team must cover all qualifications 1 to 7 listed above.

Regional experience is required for the key experts. National experience and / or and fragile state experience in the key expert team or in additional team members (non-key experts) would be desirable.

Experience with strategy formulation in telecommunications environments where common carrier services are not available is desirable. Experience should be confirmed for overcoming the challenges of operating in environments with limited resources (e.g., Internet access and power) maintaining security and compliance with dispersed offices and teams.

Industry certifications e.g., CISA, CGEIT, TOGAF, CISCO, ITILv4, CISM, CISSP, CRISC, PMP, PRINCE 2, and ISO standard certifications is desirable.

Excellent written and verbal communication skills (English) is required.

Three Key Experts are indicated as a minimum requirement; however, the Bidder may propose a single individual to cover skills sets 1 to 5 above and a second expert for skill set 6 and 7. National experience should be included in the team.

Key Expert Qualifications

Key Expert 1 and 2:

Either as two persons or one, the experts shall have applicable, deep experience in public sector revenue domain and tax and customs application software over at least ten recent years.

Key Expert 1 with this applicable, deep, recent, and long-term expertise in tax administration domain and application software will be the team leader.

Key Expert 2 shall have this applicable, deep, recent, and long-term expertise in public sector customs domain and application software.

Between them, Key Expert 1 and 2, must have experience in all areas 1 to 5 above, including application and business processes for a non-core process of revenue administration.

Both Key Expert 1 and 2 shall have regional experience in comparable roles.

It is preferred that these Key Experts have a bachelor's degree (higher degree, e.g. MBA, preferred) from a recognized university in business administration or a field of study related to revenue administration.

As mentioned, a single individual can cover both key expert 1 and 2 roles. Note however, the combined level of effort for the roles shall not be reduced if one individual possesses all necessary qualifications.

Key Expert 3:

This individual shall be the ICT technical infrastructure expert and shall be directed by Key Expert 1.

Key Expert shall ensure there is perfect consistency between the business domain / application strategies and the technical infrastructure strategies and between the strategies and the policies to be defined.

This individual shall have at least ten years' experience in roles relevant to this assignment demonstrating experience in both skill sets 6 and 7. This may be as an ICT technical infrastructure consultant documenting ICT strategy for a public sector revenue administration or in an executive position in a public sector revenue administration with practical experience in ICT technical infrastructure strategy formulation.

Key Expert 3 shall have regional experience in comparable roles.

Key Expert 3 shall have as a minimum a bachelor's degree (higher degree preferred) from a recognized university in Computer Science, Engineering or Information systems or related field.

Non-key experts

As mentioned, the Consultant may need to include one or more individuals for national and / or fragile experience. In the event, that team proposed includes a non-key expert, the individuals must have a depth of demonstrable experience in at least one of the skills sets 1 to 6 listed above.

Consultant requirements: The Bidder must be either incorporated entity or a JV of incorporated entities. The Bidder shall have executed successfully at least two contracts within the past ten years, at least one of which within the past five years, for related assignments for ICT Strategy formulation for core processes for a public sector revenue administration. Reference site details and contacts must be given.

VII. Reporting Requirements and Time Schedule for Deliverables

The main deliverables for this TOR shall be as shown below. The timing indicated is the expected delivery from the start of the assignment, however, the bidder should propose a timeframe according to its assessment of the requirements.

Item	Deliverable	Timing
1	Inception Report	+1 week
2	Draft ICT Strategy	+4 weeks
3	Presentation of Draft ICT Strategy	+5 weeks
4	Final ICT Strategy	+6 weeks
5	Project and Initiative Profiles – draft	+8 weeks
6	Project and Initiative Profiles – final	+9 weeks
7	ICT Policies – draft	+11 weeks
8	ICT Policies – final	+12 weeks
9	Final report (documenting the process and performance and indicating any suggested follow-up activities).	+12 weeks

All reports shall be delivered in soft copy.

All reports shall be delivered to the NRA Management.

In addition to the main deliverables, Key Expert 1 shall prepare a brief (1-pager) progress status summary to the NRA Executive Management team each fortnight beginning week 3 and ending week 11.

Client's Input and Counterpart Personnel

The Client will facilitate the work of the Consultant. The Client will provide:

i) Letters and related assistance for visa and other matters needed for entry into South Sudan and the activities of the Consultant in-country

ii) Air-conditioned office space, desks, and chairs suitable for desk-work for a small team (nominally for 3 persons concurrently)
[The Consultant is required to make its own arrangements for office equipment and telecommunications and all such related matters.]

iii) Entry-access to NRA offices and officers
[The Consultant is required to make its own arrangements for transport around Juba.]

iv) Facilitation for meetings with other stakeholders

v) Access to NRA documentation that is relevant to the assignment (in soft-copy when available)

The Client will provide professional, senior, counterpart personnel across the whole NRA organization necessary for successful conduct of the assignment during the research and presentation / review stages. The Consultant's demands on these personnel shall be reasonable.

For the duration of the assignment, the Client shall appoint a senior counterpart person who will facilitate access to other NRA and stakeholder persons, schedule meetings and presentations, and send reminders regarding meetings, presentations, etc. to the other NRA and stakeholder persons.