Terms of Reference

COBIT 19, NIST CYBERSECURITY FRAMEWORK USING COBIT & A DIGITAL TRANSFORMATION STRATEGY

Country: Zambia and Zimbabwe
Reference No**: ZRA-ICT-04-2023**
Assignment Title: COBIT 19 IMPLEMENTATION FOR ZAMBEZI RIVER AUTHORITY

1. **The Authority**

The Zambezi River Authority ("**the Authority**") is a corporate body jointly and equally owned by the Governments of Zambia and Zimbabwe ("**Contracting States**") and is mandated with the management of the Kariba Complex and the stretch of the Zambezi River (from Kazungula to Kanyemba) forming a common border between the two Contracting States.

2. **Background**

The Authority has a contemporary ICT Business Applications, Hardware, Network and Security Systems infrastructure. The said ICT Systems have a hybrid deployment comprising of on premise and cloud hosted systems .The main technology vendors currently in use are Cisco, Microsoft, Riverbed ,Huawei, Riverbed , Kaspersky and SAP. Over and above the Authority has Metropolitan fibre links in Lusaka Kariba and Harare and has WAN Link from Harare to Lusaka and is currently working on Expanding its WAN to remote areas of Zambia and Zimbabwe where it operates Hydrometeorological stations. The Authority also has a website(www.zambezira.org),facebook page, YouTube and twitter handle. The following documents guides the ICT operations ICT Plan ,Corporate Strategy ,Disaster Recovery Document and ICT strategy document. Thus the Authority has

to some extent implemented some of the provisions of the assignment but not in full and not in a structured manner.

3. Scope of the Assignment

The scope for consulting services ("the Services") include;

- Review and assess the current ICT Environment & cybersecurity posture, Governance and Digital Strategy
- Develop a Control Objectives for Information and Related Technologies (COBIT), National Institute of Standards & Technology (NIST) cybersecurity framework and digital transformation strategy plan that will include objectives, scope, methodology and schedule,

4. Specific Objectives

4.1 Overall Objectives

a. Provide a common language for ICT professionals, Authority's Management and Internal Audit to communicate with each other about IT controls, goals, objectives and outcomes.
b. Proper alignment of all business and IT-related strategies.
c. Ensure that IT investments are being prioritized in a way that helps the Authority to achieve its objectives without incurring additional IT risk.
d. Provide a "prioritized, flexible, repeatable, and cost-effective approach" to **cybersecurity** risk
e. Assist the Authority to;

- Identify which assets need protection.
- Implement appropriate safeguards to protect the identified assets.
- Implement appropriate safeguards to detect security threats and incidents.
- Develop techniques to mitigate the impact of these incidents.
- Implement processes to recover from cyberattacks and restore business-as-usual

f. Assist the Authority to integrate digital technology in all areas of its operations in order to deliver value to its stakeholders.

4.2 COBIT

a. Guide the Authority in using the seven (7) steps (COBIT standard) in order to customise COBIT 2019 for the Authority's business.

    i. Identify stakeholder needs.
    ii. Identify enterprise goals (picked up from the ZRA's Corporate Strategy) and alignment goals.
    iii. Identify the Governance and Management Objectives
    iv. select and customize goals and metrics for enterprise and alignment goals.
    v. Select and customize the components of the governance and management.
    vi. Prepare customized COBIT Contents and integrate them into enterprise practices.
    vii. Implement performance and monitoring measures to confirm results and take remedial action.

b. Assist the authority to implement COBIT by following the COBIT implementation phases.
c. Determine the Authority's ICT Maturity and proffering the best remedial action.
d. Assist the Authority to attain COBIT certification.
e. Assist the Authority in understanding the various elements of COBIT 2019, in particular the Core Model and the eleven (11) Design Factors, and their impact.

4.3 NIST cybersecurity framework Using COBIT 19

a. Assisting the Authority to align and adopt the NIST framework.
b. Assist the Authority in coming up with activities in order to comply with the NIST Framework using COBIT 19.
c. Mentor the Authority on the different facets of the NIST framework and adoption strategy.
d. Provide a detailed training plan .

4.4 Digital Transformation Strategy in line with COBIT 19

To develop a strategy that will assist the Authority to integrate digital technology in all areas of its operations in order to deliver value to its stakeholders.

5. Consultant Deliverables/Outputs

The Consultant will be required to deliver the following.

No	Deliverable	Timelines
1.	Inception Report	Within 20 calendar days from commencement date • The Report must contain a brief review and summary of existing situation and information relating to project progress. • Work plan including indicative planning, description of priorities identified.
2	Customised COBIT Framework for the Authority with relevant Governance Structures	Within 45 calendar days from commencement date
3	Customised and COBIT integrated NIST Framework for the Authority	Within 60 calendar days from commencement date
4	Digital transformation strategy for the Authority	Within 90 calendar days from commencement date
5.	Monthly Reports	Every Month– 7 calendar days after completion of preceding Month • Consolidated Progress Report detailing key issues and constraints affecting project implementation, summary on project progress and performance indicators, milestone achievement, key risks identified and proposed/applied risk mitigation, recommendations for improved/accelerated project implementation. • Best practice to be adopted and lessons learned • Recommendations/suggestions and priorities for the next period of the assignment. • Reports should also include recommendations on aspects such as quality management and risk management systems within the Authority
6.	Draft Final Report	Within 120 calendar days from commencement date

		One month prior to Contract completion date • Summary of all important matters raised by previous reports, observations on project progress and lessons learnt. • Recommendations for continual improvement of the Authority's ICT Governance, Security Framework and Digital Transformation
7.	Final Report	Within 10 calendar days after receiving comments to Draft Final Report. • Summary of all important matters raised by previous reports, observations on project progress and lessons learnt. • Recommendations for continual improvement of the Authority's ICT Governance, Security Framework and Digital Transformation.

6. Type of Contract and Assignment Timeframe

This shall be a **lumpsum contract** and the Consultant shall perform the tasks indicated in 5 above over a maximum period of 12 months.

7. **Estimated Experts Time Inputs**

The estimated level of effort or Experts time inputs required to execute the assignment is **six (6) man months**.

8. Payment Milestones

Arising from the Deliverables/Outputs, payments to the Consultant shall be paid as follows,

No	Deliverable	Timelines
1.	1st Payment 15% of the contract amount	After production and approval by the Authority of the inception Report
2.	2nd Payment 25% of the Contract Amount	Payment will be done upon production and approval by the Authority of an Authority aligned COBIT Framework

3	3rd Payment 20% of the contract Amount	Payment will be done upon production and approval by the Authority of an Authority COBIT aligned NIST Framework
4	4th Payment 20% of the contract amount	Payment will be done upon production and approval by the Authority of an Authority aligned Digital Transformation Strategy and training for 5 days.
5	5th and Final Payment 20% of the contract amount	Payment will be done upon production and approval by the Authority of the final completion report.

9. Data to be provided by the Authority

The Authority will share the following data/reports with the successful firm:

- ICT Strategy
- ICT Operational Plan
- ICT Policy
- Disaster Recovery Plan
- Corporate Strategy Document (available on the website)

10. Location f the assignment

The assignment will take place primarily at the Head office site in Lusaka , Zambia and within the offices of the Zambezi River Authority in Kariba and Harare . ZRA will provide suitable office space as required to carry out the assignment by the Consultant.

11. Tools to be provide by the Consultant.

The Experts must provide their own computer hardware and software required to perform the assignment.

12. Qualifications of the Firm and Experts

12.1 Firm Experience

The firm should have at least fifteen (15) years' experience in the provision of the said consultancy services of similar nature and must have successfully conducted at least three (3) similar assignments in the last seven (7) years.

12.2 Key Experts Qualifications, Experience and Competences

a. LEAD EXPERT

- First Degree in Computer Science, Information Systems, electronic systems or related field
- Advanced Degree in Computer Science, Information Systems, electronic systems or related field
- The Expert must have a minimum of ten (10) years of post-graduate relevant professional experience specifically on COBIT, NIST and Digital Transformation & ICT Service Management
- The Expert must have implemented at least three (3) COBIT assignments. COBIT assignments within a public sector organisation an added advantage.
- The Expert must have implemented at least two (2) NIST assignments. NIST assignments within a public sector organisation an added advantage.
- The Expert must have implemented least two (2) Digital Strategy Transformation assignments. Digital Strategy Transformation assignments within a public sector organisation an added advantage.
- The Expert must have an Advanced Degree in Computer Science, Business Administration, Engineering, Business or equivalent.
- Certifications in Cobit Implementation (Foundation, Design, and Implementation), Assessment
- Security Certification
- Relevant Membership in a Professional Body.
- Written and oral fluency in the English language is required.
- Good understanding of risk management.
- Written and oral fluency in the English language is required.

b. ASSOCIATE EXPERT

- Degree in Computer Science, Information systems, Data Science informatics or related field
- Certification in Project Management
- At least five (5) years in implementing COBIT, NIST/ISO27000, ICT Digital Transformation
- Evidence of having implemented at least two (2) projects involving COBIT, NIST and ICT digital transformation
- Security Certification
- Certification in ICT service Management

13. Experts Key Competences

- Strategic thinking and planning skills
- Decision making skills
- Operational effectiveness
- Influence **and** interpersonal effectiveness
- Innovative
- Effective communication

14. Reporting

All deliverables will be:

- in English;
- of high quality, well written, concise and to the point;
- confidential and prepared in electronic version both in Word and PDF formats and be provided to the Authority.

15. Training

The firm must provide a detailed training program for the Authority in line with the guidelines of COBIT, NIST and Digital Transformation. The firm must provide Certified Training to the Authority's six ICT employees in COBIT, NIST and Digital Transformation.