TERMS OF REFERENCE
(CONSULTING SERVICES – FIRM SELECTION)

Assignment Title:
INTEGRATED CONSULTING ENGAGEMENT FOR THE SURVEILLANCE AUDIT PREPAREDNESS ON INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) - ISO 27001 - INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS), ISO 20000 - INFORMATION TECHNOLOGY SERVICE MANAGEMENT SYSTEM (ITSM), ISO 22301 – BUSINESS CONTINUITY MANAGEMENT (BCM)
Reference No: NG-DBN-231086-CS-CDS

I. Context

The Development Bank of Nigeria Plc. ("DBN") was established in September 2014 to provide medium to long term financing for the Micro, Small and Medium scale Enterprises (MSMEs). The objective is to alleviate financing constraints faced by MSMEs and small Corporates in Nigeria through the provision of financing and partial credit guarantees to eligible financial intermediaries on a market-conforming and fully financially sustainable basis.

In addition, DBN through its subsidiary Impact Credit Guarantee Limited (ICGL) provides partial credit guarantees on loans made to eligible Micro, Small and Medium Scale Enterprises (MSMEs) and small corporates by Participating Financial Institutions (PFIs) in Nigeria.

To support the DBN's core values of sustainability and transparency, the DBN carried out a recertification exercise and obtained its recertification in 2021 in the following relevant International Organisation for Standardization (ISO) standards relating to management of information security, service management quality and business continuity in providing wholesale term lending to Participating Financial Institutions (PFIs) to address the major financing challenges facing Micro, Small and Medium Scale Enterprises (MSMEs) in Nigeria:

a) ISO 27001 – Information Security Management System (ISMS),
b) ISO 20000 – Information Technology Service Management System (ITSM),
c) ISO 22301 – Business Continuity Management (BCM),

As required by the ISO, the certification body conducts annual surveillance audits and re-certification exercises every three years. A recertification in the Standards were obtained by the DBN in Q4 2021, hence, a surveillance audit will become due in Q4 2022. The project's goal is to prepare DBN for the surveillance audits of the ISO standards (ISO 27001, 20000, and 22301), and facilitate the audit by the surveillance body.

II. Objective

The purpose of this assignment is to:

a) Assist Development Bank of Nigeria Plc. (DBN) in preparation for the surveillance audit in the International Organization for Standardization (ISO) standards 27001, 20000, and 22301.

III. Scope of Work

The broad Scope of Work (SoW) would be as follows:

1. Product Management Plan
   The Consultant shall develop and maintain a Project Management Plan using open-source tools or Microsoft Project. The Project Management Plan will identify:
   a) Goals and objectives.
   b) Key steps and milestones to achieve stated objectives.
   c) Implementation timelines.
   d) Consultant's Project Team members, roles and responsibilities.

   The Project Management Plan will include prioritized new activities and recommended action steps.

2. Gap Assessment
   The Consultant shall produce a detailed gap assessment report which upon closure prepares DBN for the surveillance audit. The gap assessment shall include a review of the current status of DBN's policies and processes.

3. Assisted Treatment of Gaps
   The Consultant shall work with the Bank's personnel to treat the identified gaps and provide documentation that will be used to maintain or improve on the alignment of business operations with the standards.

4. Data Mapping and Inventory Review
   The Consultant shall review the Data inventory and mapping which details the entire Bank's data lifecycle for completion and accuracy.

5. Surveillance Audit Assistance
   The Consultant shall provide guidance and support on the surveillance audit of DBN against the standards and conduct the following activities:
   i) Conduct a refresher course on the Business Continuity Management System (ISO 22301:2019) for the Risk Department and Internal Audit Unit
   ii) Conduct Enterprise Business Continuity Test and Exercise
   iii) Conduct Enterprise Vulnerability Assessment, Penetration Testing and Remediation support once a year. This shall include internal and external network

layer testing, internal and external application layer testing, security configuration review, and social engineering

iv) Conduct an enterprise IMS awareness program

v) Prepare the client for the IMS surveillance audit.

IV. Deliverables and Timelines

The Consultant is expected to submit a detailed Project Management Plan and a corresponding Work Plan, alongside a technical proposal. These will be reviewed and agreed on before contract signing.

In line with the scope of work in Section III above, deliverables to be provided by the Consultant include:

a) Gap Assessment: Commence gap assessment immediately after contract signing . Gap assessment report to be provided two (2) weeks post contract signing.

b) Assisted Treatment of Gaps: Treatment of gaps to commence immediately after approval of gap assessment report. Consultant is expected to provide documentation that will be used to maintain or improve on the alignment of business operations with the standards. Documentation is expected six (6) weeks post contract signing.

c) Surveillance Audit Assistance and Data Inventory and Mapping review. This phase is expected to commence two months after contract start date and after treatment of gaps. Surveillance audit to last for five working days. The Consultant is expected to deliver on the refresher course on the Business Continuity Management System (ISO 22301:2019) for the Risk Department and Internal Audit Unit;. Deliver on the Surveillance Audit report from the certification body and the first VAPT report; deliver on other activities as contained in the Scope of Work, Section 3(4) above.

d) Delivery of final audit report and certificate (where applicable), including other deliverables as stated on the contract. All deliverables are expected to be concluded within 11 weeks post contract signing.

In addition to the above, the Consultant will be required to prepare and submit written bi-weekly progress reports and formal monthly status reports as part of the Project Management Plan.

Monthly status reports shall include a description of progress made during the reporting period; outstanding issues and recommendations for resolution; deliverables completed during the reporting periods; summary of risks and impact identified and identification of the action and person(s) responsible for mitigating the risk and resolving problems.

V. Time Frame

The proposed duration for this project is 3 – 6 months.

VI. Deliverables and Payment Schedule

Payment Terms	Deliverables	Timeline	Percentage Payment
First Payment	Submission and approval of Gap Assessment Report	2 weeks post contract signing	10% of the total payment
Second Payment	Documentation regarding Assisted Treatment of Gaps	6 weeks post contract signing	20% of the total contract sum
Third Payment	After delivery of the surveillance audit report from the certification body and the VAPT report.	2 weeks after commencement of surveillance audit	50% of the total payment
Final Payment	At the full completion of other deliverables, delivery of final audit report and certificate (where applicable) from the Certification Body.	1 week after delivery of draft surveillance audit report and VAPT	20% of the total payment

VII. Selection Criteria

Consultants shall be selected based on the following criteria:

- Minimum of 5 years demonstrated experience with similar projects related to information security management, vulnerability management, risk management and business continuity management delivered to financial institutions. With proven affiliations with ISO certification bodies.
- Demonstrated ability to deliver on the proposed assignment with expertise in network security and penetration testing.
- Demonstrated ability and experience in preparing standardized analytical reports. Experience should include a minimum of 2 similar assignments with financial institutions.

Interested Consultants should provide information on the following:

a) The firm's general experience in the field of assignment.
b) The firm's track record.
c) The qualification and experience of the personnel proposed for the assignment.
d) The proposed work plan methodology and approach in response to suggested terms of reference

Key Staff Requirements:

- **Team Leader:** Information security expert with at least 10 years' experience in information security and information systems management as well as proven track record of successfully delivered projects in financial institutions. The team leader should also demonstrate knowledge of the ISO standards and affiliations with ISO certification bodies.

- **Team Members:** Bachelor's degree and at least 5 years professional experience of working in information technology and security.