NATIONAL PENSIONS REGULATORY AUTHORITY

REQUEST FOR EXPRESSION OF INTEREST (EOI)

CONSULTANCY SERVICES FOR THE PROVISION OF ISO CERTIFICATION

Ref. PN6/21-08-2023

The National Pensions Regulatory Authority (NPRA) intends to apply part of its Internally Generated Funds (IGF) to fund the assessment and certification of ISO 27001:2013 which is an international standard that outlines the best practices for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

Background

This has become necessary due to the growing need for information security in the face of increasing threats and vulnerabilities in the digital world. The purpose is to help the NPRA identify, assess, and mitigate information security risks, and to implement controls to protect its information assets from unauthorized access, use, disclosure, alteration, destruction, and theft to ensure the confidentiality, integrity, and availability of its information assets.

Further, based on the Information Communication Technology Steering Committee of the NPRA approval, recommended to adopt such standard that will intensify its efforts on certifying NPRA's IT processes to International Standards for Organization (ISO) by working on these processes. One of these is the Information Security Management Systems (ISMS) certification.

Considering that the processing of NPRA transactions is largely dependent on its computerized system, it is essential for NPRA to ensure not only the quality of service to the pension sector stakeholders and the general public but also provide a secured information system that will promote data integrity, manage information risks, and increase defense from cyber-attacks that attuned to IT standards and industry best practices. Thus, this project will suffice the need on the information security assessment and ISMS audit pre-compliance of the Authority.

Objectives of assignment

The objective of the assignment is to successfully implement the following:

1) To assess the current information security management and environment of NPRA and to identify risks and opportunities.
2) To develop and implement the standard-based management system for information security following ISO 27001:2013 ISMS framework to the following areas, but not limited to:

i. Information Security Policies;
ii. Organization of Information Security;
iii. Human Resources Security
iv. Asset Management
v. Asset Control
vi. Cryptographic
vii. Physical & Environmental Security
viii. Operations Security
ix. System Acquisition, Development & Maintenance
x. Supplier Relationship
xi. Information Security Incident Management
xii. Business Continuity Management;
xiii. Risk, Incident, Problem and Change Management;
xiv. Compliance Management:

To conduct Vulnerability Assessment and Penetration Testing (VAPT) in the NPRA networks and information systems;

4) To conduct an NPRA-wide information security awareness and ISMS certification training programs;
5) To ensure the objectives, processes and procedures related to risk management and improvement of information security that will provide results are established in-line with the globally standardized policies and objectives of the NPRA; and
6) To establish internal control mechanisms that are applicable to NPRA operations for the protection of data and information.

Scope of Work/Services

The engagement shall cover the NPRA's business processes and its corresponding information systems, software, communication systems, and network infrastructure, its management related to office applications, to implement the IT services provided to internal and external clients. The Consultant shall:

1. Assess the current state of the Information Security Management of NPRA;
2. Review documents and records required by ISO 27001:2013.
3. Conduct Vulnerability Assessment and Penetration Testing (VAPT) in the NPRA domain networks and information systems.
4. Design and develop an effective and easy-to-use ISMS implementation plan that can be successfully implemented.
5. Conduct workshops, trainings, and meetings to facilitate completion of mandatory and other necessary documents based on the ISMS Guidelines.

NATIONAL PENSIONS REGULATORY AUTHORITY

REQUEST FOR EXPRESSION OF INTEREST (EOI)

CONSULTANCY SERVICES FOR THE PROVISION OF ISO CERTIFICATION

Ref. PN6/21-08-2023

6. Provide support and assistance in the implementation and monitoring of the established ISMS.
7. Provide assistance towards compliance with the auditing requirements under the ISMS.
8. Conduct readiness and pre-certification assessment.
9. Provide audit assistance for ISO 27001:2013 ISMS certification.
10. Consulting firm must ensure that service provider's representatives are physically and mentally fit to perform the work and compliant with NPRA health protocols.
11. Conduct assessment into required training needs for NPRA IT Unit staff on ISO 27001 Management.

Duration of the Assignment

The expected duration for the execution and handing over of the assignment shall be for a period of four (4) calendar months after contract signing.

The National Pensions Regulatory Authority now invites eligible consultancy firms to indicate their interest in providing the services. Interested consultants must provide information indicating that they are qualified to perform the services (brochures, description of similar assignments, experience in similar conditions, availability of appropriate skills among staff, etc.)

A consultancy firm will be selected under the Consultant Qualification method in accordance with the procedures set out in the Public Procurement Act, 2003 (Act 663) as amended, and shall meet the following requirement.

- Valid Business Registration Certificate with up-to-date renewal receipt.
- Valid GRA Tax Clearance Certificate.
- Valid SSNIT Clearance Certificate.
- Valid VAT Registration Certificate.
- Valid PPA Suppliers Registration Certificate
- Cyber Security Service Provider License
- Relevant Experience of Firm in ISO/IEC 27001
- Availability and Experience of relevant key staff

The shortlisting criteria shall be:

S/N	CRITERIA	POINTS
1	**Validity of Statutory Documents** (Bus. Reg. Cert, PPA Cert, Tax Clearance Cert, SSNIT Clearance, Cyber Security Cert. etc)	15
2	**Experience of Relevant Key Staff**	20
3	**2021 & 2022 Audited Accounts**	5
4	**General Experience** No of years in doing business and Annual turnover the last 3 years	20
5	**Specific Experience** Previous experience in carrying out similar assignment including demonstrated experience in similar assignment	30
6	Experience in Information Security Management	10
Total		**100**

Only shortlisted firms who obtained at least **70 points** will be issued with the Request for Proposal (RFP) to submit their Technical and Financial Proposals.

Expression of Interest in three copies (**1 original, 2 copies**) must be delivered to the address below by 4:00pm on **Wednesday September 6, 2023.**

Interested consultants may obtain further information at the address below from 8:30am to 4:30pm.

Any request for clarification on the EOI should be sent via email below not later than **Wednesday August 30, 2023.**

Address: National Pensions Regulatory Authority
Post Office Box GP22331
SU Tower, 9th Floor
Ridge, Accra
Email: procurement@npra.gov.gh
Tel: 0302 – 968692/0302 968693

Website: www.npra.gov.gh , e-mail: info@npra.gov.gh

"Ensuring Retirement Income Security"