بسم الله الرحمن الرحيم

Pension Office

INVITATION FOR SUBMISSION OF PROPOSALS TO PROVIDE ISO 27001:2013 CONSULTANCY SERVICE

ADDITIONAL INFORMATION ISSUED IN RELATION TO ANNOUNCEMENT

REF: 216-MPAO/IUL/2019/16, DATED 23RD MAY 2019

1. SUMMARY

Maldives Pension Administration Office (Pension Office) has been enhancing the Information Security Management System (ISMS) and a multitude of security controls and measures have been put into operation since 2017. As part of the organization's strategy and commitment to foster information security, Pension Office is looking for a consultancy firm ("the Firm") to provide professional services leading to certification for the ISO 27001:2013 standard.

The Firm shall provide expert advice and assistance to Pension Office to revamp and implement ISMS based on the latest version of the ISO 27001 standard. In addition, the Firm shall provide an onsite internal audit service to determine the readiness of Pension Office for the initial certification assessment scheduled to commence by last quarter of 2019.

Further, the Firm shall provide onsite advisory and support to Pension Office throughout the course of formal assessment to be conducted by a Certification Body. The scope of service is detailed in this document.

Parties interested in providing this service shall submit Expression of Interest (EOI) by 30th May 2019 by emailing to **proposals@pension.gov.mv** and further submit required proposal before 12th June 2019.

2. PROPOSED SERVICES

There are three parts to the required services under this engagement.

2.1. PART A - Consultancy Services

Proposed services should include, but are not limited to the following:

- Perform a gap analysis in order to assess and evaluate the controls to be implemented to achieve ISO 27001:2013 certification and accreditation.

- Review existing information of Pension Office pertaining to security controls, policies, processes and any other established procedures on managing risk and improving information security to deliver results in accordance with the organization's overall policies and objectives.

- Scoping of certification project and documenting the scope as per ISO 27001:2013 certification, detailing the functional areas and processes to be covered in the certification scope.

- Identify the information assets of Pension Office, it's ownership, classification of assets and prepare information asset registers.

- Define and document the Risk Assessment Methodology for risk identification, mitigation and treatment.

- Conduct a comprehensive Risk Assessment across all functions and processes covered under the scope of ISMS for Pension Office, prepare and present the Risk Assessment report to the management.

- Provide recommendations to Pension Office internal team and senior management for mitigating high risks identified during the Risk Assessment.

- Implement an ISMS based on the requirements of ISO 27001:2013.

- Review the current Organizational Structure and advise/modify to create an environment where policies, procedures and processes to manage and monitor regulatory, legal, risk, environmental and operational requirements are understood and inform the management of security risks.

- Define all ISO 27001:2013 roles and responsibilities and mapping them to existing business departments or positions according to the approved Organizational Structure.

- Define and develop required information security policies and procedures for Pension Office.

- Define and create an evaluation method and metrics of the ISMS and the implemented controls. The plan should:

    - describe the goal of measurement objective;
    - define methods of collecting performance data;
    - define the frequency and method of monitoring;
    - define performance metrics, KPIs and dashboards for implemented security controls.

- Conduct ISO 27001:2013 awareness sessions to Pension Office staff.

2.2. PART B - Internal Audit Service

Prior to the official assessment for certification, an onsite internal audit should be performed to determine the readiness of the in-scope services for the formal assessment. Activities during the onsite internal audit should include, but are not limited to the following:

- Assess the ISMS and related activities, processes, procedures and documentations.

- Conduct an internal audit by an independent team that did not participate in the ISMS implementation.

- Assist Pension Office team and provide consultancy on the Risk Treatment status, closure of Internal Audit findings, and other matters prior to the certification.

- Benchmark against the ISO 27001:2013 standard and identify any non-conformity.

- Provide assistance and support on remediating all non-conformities, including the revision of all necessary documentation.

2.3. PART C - Onsite Support during Formal Assessment

The Firm should provide onsite advisory and support throughout the course of formal assessment of the Certification Body. This should include, but are not limited to the following:

- Attend interviews and site-visits with the external assessors.
- Assist in the identification and collection of audit evidence.
- Follow-up on queries raised by the Certification Body.

3. ELIGIBILITY CRITERIA

The bidder should possess the requisite experience, resources and capabilities in providing the services necessary to meet the requirements, as described in this RFP. The Bid must be complete in all respects and should cover the entire scope of work as stipulated in this document. Parties who does not meet the Eligibility Criteria will not be considered for further evaluation.

3.1. Previous Experience Requirements

The Firm responding to this RFP shall demonstrate their capabilities and experience in providing similar services and similar engagements especially in the financial sector. These services and engagements must be performed by the Firm during the last five (5) years (minimum 3 similar successfully accomplished projects are required). Furthermore, the Firm shall demonstrate the following specific capabilities:

- Experience in designing, developing, implementing, and successful certification assistance in ISO 27001:2013

- Experience in conducting full ISO 27001:2013 internal audits.

- More than 5 years in the field of information security, governance, risk and compliance in the region of operation.

3.2. Qualifications of the Consultants

The Firm should have minimum four (4) resource personnel with more than three (3) years experience in ISO 27001:2013 implementation and internal auditing. The proposed team must also be certified in at least two (2) of the following certifications/professional qualifications.

- ISO-27001 Lead Auditor (LA)/Lead Implementer (LI).
- Certified Information Systems Auditor (CISA).
- Certified Information Security Manager (CISM).
- Certified Information Systems Security Professional (CISSP).

4. INSTRUCTIONS TO THE BIDDER

Technical Bid and Financial Bid must be submitted giving full particulars in two separate sealed envelopes at the address given below, on or before the dates mentioned below. All envelopes should be securely sealed and stamped.

The Technical Bid should not contain any price information. The Financial Bid should give all relevant price information including all applicable taxes and should not contradict the Technical Bid in any manner.

All the envelopes must be superscribed with the following information:

- Type of Proposal (Technical or Financial)
- Tender Reference Number
- Due Date
- Name of Bidder
- Name of the Authorised Person

Address for Communication:

For the purpose of clarification of doubts on issues related to this RFP, please send queries to **proposals@pension.gov.mv** by 5th June 2019.

Important Dates:

Expression of Interest:	30th May 2019
Enquiries:	5th June 2019
Bid Submission Date:	12th June 2019 before 14:00

Proposal Submission

Proposal must be sealed and submitted in person on **Wednesday, June 12, 2019, (14:00)** and addressed to;

Maldives Pension Administration Office
City Square, 8th Floor
Chaandhanee Magu
Male`
Maldives

5. BID EVALUATION

Weights allocated to the Technical and Financial bid are:

80% for the Technical Bid
20% for the Financial Bid

Bidders scoring 70% or more from the Technical Bid evaluation will qualify and the Financial Bid of only qualified bidders will be opened.

After Technical Bid evaluation, the Pension Office shall notify those bidders whose bids did not meet the minimum qualifying mark or were considered non-responsive

to the RFP, indicating that their Financial Bid will be returned upon completion of the selection process.

The Pension Office shall simultaneously notify bidders who have secured the minimum qualifying mark, indicating the date and time set for opening the Financial Bid and stating that the opening ceremony is open to those bidders who choose to attend.

5.1. Technical Evaluation

The bidder will have to give a presentation on the following points as a part of the technical evaluation.

- Process approach for ISO 27001:2013 design and Implementation.
- Risk Assessment process approach and methodology.
- ISMS development activity details.
- Pre-audit assessment process plan and execution.
- Statement of Applicability: approach and completion.
- Deliverables.
- Project timeline and completion plan.
- Consultancy Team details including qualifications, experience, etc.

The Technical Evaluation will be based on the following broad parameters.

No	Technical Evaluation	Expected Response	Marks
1	Proposal on Scope of Work (requirements) as specified in the RFP.	Proposal Document	20
2	Presentations on the skills, services provided on ISO 27001:2013 Certification.	Presentation will be scheduled and communicated to all bidders.	20
3	Customer references submitted by bidder	Document detailing customer references.	20
4	Documentary evidence for the scope of work already executed by	Documentary Evidence.	20

	the bidder, more weightage will be given for ISO 27001:2013 executed work.		
5	Experienced and skilled professionals having certifications (e.g. ISO 27001:2013 Lead Auditor, CISA, CISSP, CISM and CEH) to carry out ISO 27001:2013 certification implementation at Pension Office. Comparison of skilled resources will be done based on the number of resources with desired certifications.	Summary Document and copy of individual certificates. Please mention the number of professionals and their certifications in summary.	20
	Total		**100**

5.2. Financial Evaluation

Evaluators of Technical Bid shall not have access to the Financial Bid until the Technical evaluation is concluded.

The formula for determining the Financial Score (FS) is as follows:

FS = 100 X LF/F, where FS is the Financial Score; LF is the lowest priced financial bid and F is the price of the bid under evaluation.

Bids will be ranked according to their combined technical and financial scores using the weights (T = the weight given to the Technical Bid: P = the weight given to the Financial Bid). The combined technical and financial score, S, is calculated as follows: **S = TS x T % + FS x P %**. The Firm achieving the highest combined technical and financial score will win the bid.

6. TIMEFRAME

The primary objective is to enable Pension Office to obtain ISO 27001:2013 certification before the end of 2019. Accordingly, the Firm would carry out a comprehensive study of the existing systems and procedures, documentation etc. in the set-up identified for certification and should harmonize them with ISO

standards, culminating in the Certification. Accordingly, the entire project should be completed within six (6) months starting from the contract signing date.

7. PRICE AND PAYMENT TERMS

Price shall remain fixed during the contract period. There shall be no increase in price for any reason whatsoever. Therefore, no request for any escalation of the price shall be entertained.

The following payment schedule is proposed.

Milestones		**Payment %**
1	PART A - Consultancy Services	20%
2	PART B - Internal Audit Service	20%
3	PART C - Onsite Support during Formal Assessment	60%
	Total	**100%**