# Terms of Reference

**System Audit – Information Technology System of the Maldives Retirement Pension Scheme**

## I. Background

1. The Maldives Retirement Pension Scheme (MRPS) is administered by Maldives Pension Administration Office (MPAO) and supervised by the Pension Supervision Department (PSD) of the Capital Market Development Authority (CMDA) under the Pension Act (8/2009).

2. The MRPS is operated via its Information Technology (IT) system – 'Koshaaru'. MPAO has started using Google Cloud Platform since August 2017. CMDA plans to conduct an audit of the Koshaaru system in order to assess control risks, and respective preventive, detective and corrective controls within the entire system.

## II. Objectives

The objective of this Terms of Reference (TOR) is to hire a firm ('the firm') to provide a comprehensive audit and assurance of the MRPS IT System 'Koshaaru' (henceforth 'Koshaaru' or 'IT system') as detailed in the scope of services. The firm shall report on conclusions reached from its audit and recommend suitable measures for correcting any deficiencies identified during the audit process.

The contract must be completed in accordance with ISACA 'IS Audit and Assurance Standards'.

## III. Scope of services

The firm shall provide a complete audit and assurance of the entire Koshaaru system (described in section IV) with due regard to the following:

- IT performance
- Internal controls of the system
- Compliance with external requirements (laws, regulations and agreements)
- An evaluation of the governance structure of the IT system

For the above purpose, the firm shall carry out the following tasks:

**Task 1: Conduct a risk assessment of the pension system, MPAO, and the IT system:**

This task involves the auditor understanding the Maldives Pension System, the MPAO and the IT system and the associated risks. For this purpose, the auditor shall identify and assess the risks related to all processes of the pension system such as:

a. Enrolment of members
b. Contributions
c. Investment and valuation of pension assets
d. Movements in and out of portfolios (member choices)
e. Reporting: generation of account statements, fund reports etc.
f. Retirement: changing of portfolio, subsequent valuation and disbursement of benefits
g. Reconciliation of payments
h. Compliance and enforcement

i. Calculation of administrative fees, fines and penalties

**Task 2: Assess the effectiveness of preventive, detective and corrective controls associated with identified risks.**

This is inclusive of the following controls:

a. Logical access controls: verify that controls exist to ensure that only authorized users have access to the system and that the people who have access to the system do not have a segregation of duties problem with having this access.
b. Data protection: verify whether data can be accessed or changed without proper authentication and accountability.
c. Input controls: determine if there are controls in the system to ensure that only valid and correct data can be entered.
d. Processing controls: verify if controls exist to ensure that all data is processed and accurately accounted for. Ensure the accuracy of system calculations (contributions, asset values, payouts, member data etc.)
e. Output controls: verify that controls are in place to ensure that output confidentiality is maintained according to its classification level.
f. Interface Controls: verify that controls are in place to ensure that data received from other automated sources are verified as accurate before being loaded into the application.
g. Change Management and Control: determine that the processes and tools used to report, track, approve, fix, and monitor changes on the system are appropriate.
h. Contingency Planning and Backup: verify that backup and disaster recovery plan for the systems exist and is appropriately tested.
i. System Scalability: determine whether the information system and related infrastructure can adequately support anticipated growth.

**Task 3: Formulate the system audit and assurance report inclusive of the final assessment and recommendations.**

## IV. Details of the Koshaaru System

The Koshaaru system consists of the following:

| MODULES | |
|---|---|
| **0** | **System Configuration** |
| 0.1 | Configuration values |
| **1** | **Member Register** |
| 1.2 | Register New Member |
| 1.3 | Additional Identifiers or Expiry of Identifier |
| 1.4 | Member Status |
| 1.5 | Detect Automatic Retirement |
| 1.6 | Member authentication password |
| 1.7 | Maintenance of member information |
| 1.8 | Generic member search |
| 1.9 | Audit trail log of maintenance of membership records |
| **2** | **Employer Register** |
| 2.2 | Registration of employers |
| 2.3 | Data verification of employers |

| | |
|---|---|
| 2.4 | Employer authentication password request |
| 2.5 | Maintenance of employer information |
| 2.6 | Generic employer search |
| 2.7 | Audit trail log of maintenance of employer records |
| **3** | **Employment Register** |
| 3.2 | Check employment register |
| 3.3 | Register employment activity |
| 3.5 | Mandates for individual % rates for worker and employer contributions |
| 3.6 | Audit trail log of maintenance of employment records |
| **4** | **Contribution Collection** |
| 4.2 | Upload electronic SPC form |
| 4.3 | Submission of SPC using previous submitted data |
| 4.4 | Voluntary participants |
| 4.5 | CORE validation |
| 4.6 | Receipt notice and payment order |
| 4.8 | Correction of previously paid employment |
| **5** | **Payment – Reconciliation** |
| 5.1 | Electronic bank statement |
| 5.2 | Reconciliation process |
| 5.5 | Reconciled member registers |
| 5.6 | Posting employer fines for late submission of SPC |
| **6** | **MPAO Administrative Fees** |
| 6.1 | Administrative Fees |
| 6.2 | Calculate Administrative Fees |
| **7** | **Individual Retirement Accounts** |
| 7.2 | Member portfolio selection |
| 7.3 | Unitization of individual transactions and balances |
| 7.4 | MPAO ruling on portfolio change |
| 7.5 | Transfer of funds between portfolio schemes |
| 7.7 | Posting of fees for late payments |
| 7.8 | Audit trail log of maintenance of portfolio scheme selection |
| **8** | **Accounting** |
| 8.1 | External accounting |
| 8.2 | Internal accounting |
| 8.3 | Post account values |
| 8.4 | Account reporting |
| **9** | **Workflow** |
| 9.1 | Workflow configurations |
| 9.2 | Work trays |
| 9.3 | Decision component |
| 9.4 | Workflow reports |
| **10** | **Noncompliance of payment** |
| 10.2 | Detect NON declared obligations |
| 10.3 | Detect NON paid obligations |
| **11** | **Grievance – Complaint module** |
| 11.2 | Submit a complaint |
| 11.3 | Complaint resolution |
| 11.4 | Individual account correction transactions |
| 11.5 | Appeal process |

| | |
|---|---|
| 11.6 | Audit trail log of maintenance of individual accounts |
| **12** | **Claim benefits – withdrawals** |
| 12.2 | Early notification of retirement age |
| 12.3 | Submission of claim request to acquire pension rights |
| 12.4 | Register proof documentation |
| 12.5 | Register beneficiaries |
| 12.6 | Register bank details |
| 12.7 | Authorization of rejection claim request |
| 12.8 | Calculate member's account balance and Balance Control |
| 12.9 | Mapping life expectancy, member, family group |
| 12.13 | Lump sum payout |
| 12.14 | Posting of MRPS payments to Basic Pension module |
| **13** | **Asset Managers – MPAO** |
| 13.1 | Register Asset Managers |
| 13.2 | Distribution of investment account |
| 13.3 | Register Asset Manager to a Custodian |
| **14** | **NAV Accounting** |
| 14.2 | Investment fund values from Asset Managers |
| 14.3 | Calculation of NAV |
| 14.4 | Unit value of portfolio |
| 14.5 | NAV report, Authorization and Publication |
| **15** | **Reporting** |
| 15.1 | Member Individual RSA statement |
| 15.2 | Employer compliance certificates |
| 15.3 | Detailed member information report |
| 15.4 | Portfolio market performance |
| 15.5 | Management and stakeholder indicators |
| 15.6 | General operational statistics and reports |
| 15.7 | Query, search and exportable formats |
| **HARDWARE AND TECHNOLOGY** | |
| **16** | **Technology** |
| 16.1 | Web based architecture |
| 16.2 | Electronic data interchange |
| 16.3 | ODBC compliance |
| 16.4 | Single sign on |
| 16.5 | Data Base |
| 17.1 | Network security |
| 17.2 | Data integrity |
| 17.3 | Login security |
| 18.1 | General Audit Trail |
| 19.1 | Employer, member notification/alert (email) |
| 20.1 | Backup and data archiving |
| 21.1 | Online help |
| 22.1 | Document management and archiving |

## V. Schedule of tasks and deliverables

The main deliverable for this project is the "Audit and Assurance Report" which shall include the following components:

- An executive summary containing the audit objectives, scope, approach, key issues identified and overall conclusion.
- Detailed risk assessment and review of internal controls containing the observation, risk implication and recommendation for improvement of each identified issue.
- All working papers, interview notes, test results, meeting minutes and other audit evidence.

The contracting firm is required for the period from 1 April 2018 through 31May 2018.

| Main Deliverable | Deadline |
|---|---|
| Audit Plan | To be submitted during the application process. |
| Audit and Assurance Report | 31st May 2017 |

Changes can be proposed to the schedule in a manner that would aid better delivery of the project deliverables and achievement of the project milestones within the specified timeframe.

## VI. Services and facilities to be provided by the client

MPAO shall provide workspace with the following support:

- Workspace
- Access to internet and telephone
- Access to business documents
- Facilitate meetings and interviews
- Other required support services
- Onsite access to all data required for the audit (auditors shall have access to data on the premises and shall not extract any data)

## VII. Confidentiality of data

All data and information used, audited and produced during the audit is confidential. No data or other information from the audit shall be released to third parties. Data of individual members shall not be released to any party for any reason.

## VIII. Required Expertise and Qualifications

Interested firms must propose an audit team that meets the requirements stated below.

- The lead member of the team must be a Certified Information Systems Auditor (CISA) awarded by ISACA.
- At least two members with a minimum of 3 years' experience conducting Information Systems Audits for pension funds, investment funds, mutual funds, or similar financial institutions.

The audit team proposed in the application must not be changed at any point of the project without the approval of the client.



CAPITAL MARKET DEVELOPMENT AUTHORITY · MALDIVES ·