

RESERVE BANK OF MALAWI

GUIDELINES FOR PENSION ADMINISTRATION SYSTEM REQUIREMENTS

(Financial Services Act, 2010 and Pension Act, 2011)

PENSION AND INSURANCE SUPERVISION DEPARTMENT

CONTENTS

1 INTRODUCTION 3

2 PART I: MINIMUM BASIC REQUIREMENTS FOR A PENSION FUND ADMINISTRATION SYSTEM 4

2.1 Calculations 4

2.2 Reporting 4

2.3 System Administration 6

2.4 Interfacing and compatibility issues 8

2.5 System Maintenance and Support 8

2.6 Other 9

3 PART II: IT RISK MANAGEMENT GUIDELINES 9

3.1 Information Technology Governance 9

3.2 IT Risk Management Framework 11

3.3 Outsourcing IT Services 12

3.4 Acquisition, development and implementation of information systems 14

3.5 Business Continuity Management 16

INTRODUCTION

Administrators of Pension schemes face several risks including data loss or improper data management or maintenance. These risks may lead to errors and inefficiencies resulting in pension members getting wrong levels of accumulated pension benefits. It is therefore vital that administrators of pension funds must have a robust and secure information technology platform in order to perform their functions efficiently and effectively.

The following guidelines serve as minimum ICT system requirements for licensing of administrators of pension funds as well as ICT risk management requirements.

The main objective of these guidelines is to promote prudential management and administration of data/information in pension funds in order to promote safe, sound and prudent management of pension funds in Malawi. Thus ensuring data availability, integrity, confidentiality, and reliability – in usage, storage and transmission.

These guidelines are subject to review from time to time as required by the Registrar.

PART I: MINIMUM REQUIREMENTS FOR A PENSION FUND ADMINISTRATION SYSTEM

This part contains minimum requirements for a Pension Administration System (hereafter, the system). It sets the basic functionality that any pension fund administration system of an administrator should have.

1.1 Calculations

a) The system should be able to perform pension benefits calculations including:
   i. retirement benefits
   ii. partial withdrawals in line with legislation
   iii. death benefits
   iv. defined benefits including cost of pension (for DB funds)
   v. estimates for member pension benefits
   vi. distribution of aggregate return on fund investment across individual accounts
   vii. regulatory financial ratios
   viii. late payment interest including penalties and benefit escalations as may be imposed by legislation

b) The system should have the capability to load actuarial factors and rates.

1.2 Payments

a) The system should allow transfers of benefits to another fund

b) The system should have the capability to record payments of pension benefits including:
   i. withdrawals including partial withdrawals
   ii. retirement benefits
   iii. death benefits
   iv. deferred vested benefits
   v. any payment as maybe required

1.3 Reporting

a) The system should be able to produce reports including the following:

i. statements of account standing to the member with the following minimum information:-

(a) the account balance for each of employer component and member component of contributions as at the start of the financial year;

(b) amounts received and date credited of employer contributions, employee contributions, voluntary contributions and any transfers including severance due entitlement;

(c) Investment earnings credited to the employer and member portions;

(d) any withdrawals from the member's account in the form of early access to benefits or any other transfers into or out of the member's account including transfers to or from other pension funds;

(e) any charges, fees or deductions made against the account and appropriate allocation to the employer or member component;

(f) the account balance for each of the employer and member component at the end of the financial year

(g) Membership details including membership number, name, date of birth, date joined company and fund, date of retirement.

ii. Statement of pension benefits as prescribed by the payment of benefits directive

iii. up to date trail of month to month contributions

iv. up to date trail of month to month investment income

v. claim history of the fund

vi. any ad hoc statements or reports as may be requested by members, beneficiaries or the Registrar

b) The system should have a very high degree of reporting flexibility and a wide range of easily customizable pre-defined report templates with automated procedures, such as wizards.

c) The system should have the capability to tailor reports to suit regulatory needs including statutory returns

d) The system should have an ad hoc reporting capability to tailor reports to suit individuals, stakeholders. This should include reports at various levels such as fund, category based on specified criteria.

e) The system should have reporting flexibility which should include the ability to retrieve custom data sets and export them to various formats including Microsoft Word, Microsoft Excel, PDF, and Extensible Markup Language (XML).

f) The system should at a minimum also allow production of reports via crystal reporting

g) The system should also be able to produce

i. Membership movement reports
ii. financial reports
iii. Membership certificates
iv. Pension benefit payment letters
v. Exit declaration forms

1.4 System Administration

The system should;-

a) have the capability to create and maintain pension member accounts including;-

i. Enrollment of new members by unique Identifiers
ii. member metadata with at least the following details:

(a.) full name;

(b.) unique employment number/pension number/identity number;

(c.) date of birth;

(d.) member category;

(e.) pensionable emoluments;

(f.) date of joining fund;

(g.) postal and physical address; other contact details such as e-mail; telephone number(s);

(h.) take on values or transfers or past service

(i.) member nominations

b) allow setting up a range of pension scheme types, with the fund parameters based on the rules and policies of the pension funds and legislation.

c) have the capability to handle different categories of members on a pension fund i.e. be able to perform administration processes per category of members within a pension fund.

d) have capability to create and maintain system users and user groups.

e) allow definition of user roles and permissions including password requirements

f) have an audit trail which shall be regularly reviewed and shall include the following capabilities:

   i. All information created, edited, deleted or accessed in the system including time, date, user, and function operated.

   ii. Allowing access only to authorized personnel

g) Be able to handle defined contribution, defined benefit, and hybrid schemes; and programmed withdrawal functionalities.

h) have a function for financial management which should be able manage at least the following:

   i. annual financial statements,

ii. account ledgers,

iii. cash flow statements

1.5 Interfacing and compatibility issues

The system should

a) allow interface with other external systems (through technologies such as flat file, and XML) and minimise the dependency of processes on manual intervention and paper flows.

b) upload and validate imported data generated by external systems.

c) For self-administered pension funds, be compatible with standard payroll packages and Human Resources (HR) packages to enable automated contribution collection and processing; and reconciliation.

d) have ability to link directly to standard office packages such as word processing and spreadsheet package(s) that can enable mail merging and other office automation operations.

e) In respect to a) and d) above, have the capability to export valuation data.

1.6 System Maintenance and Support

a) The Administrator should ensure that there is adequate system maintenance and readily available support.

b) A system administrator should be assigned to the system.

c) A turnaround time for support should be at a maximum of 48 hours for software maintenance system

d) The Administrator shall assess the current performance and capacity of IT resources to determine if sufficient capacity and performance exist for the efficient running of the system.

1.7 Other

a) The system should allow storage and management of member of a minimum membership of 200,000 members for a minimum period of 10 years after death or retirement.
b) The system should have Document Image Processing (DIP) facilities, including the ability to display scanned images of contributor forms and other source documents as part of standard enquiry routines.
c) Ability to capture contributions offline storage media such as removable hard disks, CDs and update at a later time.
d) Flexibility to allow for enhancements

2 PART II: IT RISK MANAGEMENT GUIDELINES

This part outlines minimum ICT Risk Management guidelines for Administrators of Pension Funds.

2.1 Information Technology Governance

a) The board of directors and senior management of an Administrator should have oversight of the Administrator's information technology risk management.
b) The board of directors should be responsible for the following in respect to 2.1 a) above:
    i. The Administrator has an IT function that is capable of supporting the Administrator's business strategies and objectives;
    ii. Approval of IT risk management strategies and policies including an IT risk management framework of the Administrator;
    iii. Understanding major IT risks associated with the Administrator's business and operations and should set acceptable levels of the risks.

iv. Setting high ethical and integrity standards appropriate for effective risk management by establishing an exemplary culture that emphasises to all the Administrator's staff on the importance of IT risk management;

v. Establishment of the following in respect of IT risk management:

(a.) an IT governance structure;

(b.) Appropriate segregation of duties;

(c.) Clear definitions of roles and responsibilities in IT risk management;

(d.) Clear reporting structure/relationships;

vi. Strengthening of IT staff through training and incentive programs;

vii. Ensure appropriate provision of financial support necessary for annual IT risk management plans. The board should consider costs and benefits including issues on reputational risk, legal implications and security investment.

c) Senior management should be responsible for the following in respect to 2.1 a) above:

i. Implementing and complying with the national laws, regulatory and technical standards pertaining to the management of information systems;

ii. Periodically reviewing the alignment of IT strategy with the overall business strategies and significant policies of the Administrator, assessing the overall effectiveness and efficiency of the IT function;

iii. Ensuring that all employees of the Administrator fully understand and adhere to the IT risk management policies and procedures approved by the board of directors, and are provided with adequate training;

iv. Ensuring that pension member information, financial information, product information and information systems are protected;

v. Ensuring that IT function possess relevant academic or professional qualifications, knowledge, skills, ethics and integrity required

vi. Reporting in a timely manner to the Registrar any serious incident of information systems or unexpected event, and quickly respond to it in accordance with the contingency plan;

vii. Performing other related IT risk management tasks.

2.2 IT Risk Management Framework

a) The Administrator should establish an IT risk management framework which can be a standalone or embedded document;

b) The IT risk management framework should encompass a systematic and consistent way of managing the Administrator's IT risk, and should cover the following:

i. Roles and responsibilities in managing IT risks;

ii. Identification and prioritisation of information system/ IT assets;

iii. Identification and assessment of impact and likelihood of the current and emerging IT risks, threats and vulnerabilities on the Administrator's business;

iv. Implementation of appropriate risk mitigation measures, practices and controls;

v. Ongoing monitoring for threats and vulnerabilities and updating the IT risk strategy and framework as necessary.

c) The Administrator should develop an IT risk assessment plan and a comprehensive set of IT risk management policies that should include the following areas:

i. Information security

ii. System development, testing and maintenance
iii. IT operation and maintenance
iv. Access control
v. Physical security
vi. Personnel security
vii. Business Continuity Planning
viii. Disaster recovery
ix. an up to date IT inventory.

2.3 Outsourcing IT Services

Outsourcing involves sourcing of IT services or facilities from a single third party or multiple third party vendors within Malawi or abroad.

a) The Administrator should ensure that all contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties are set out in clear written agreements.
b) Before entering into, or significantly changing, an outsourcing arrangement, an Administrator should:
    i. Analyze how the arrangement will fit with its organization structure; business strategy; overall risk profile; and regulatory obligations;
    ii. Consider whether an outsourcing arrangement will allow the Administrator to monitor and control risk exposure associated with the outsourcing;
    iii. Conduct appropriate due diligence of the service provider's financial stability, expertise, risk assessment, facilities and ability to cover potential liabilities;

iv. Consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen on the termination of the contract); and

v. Consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several Administrators or several systems of the Administrator.

c) The Administrator should ensure that the outsourced service or facility provider grants access to its systems, operations, documentation or facilities to all parties nominated by the Administrator including the Registrar.

d) All outsourcing contracts should be approved by the Board and signed off by senior management, internal IT auditors, legal personnel and IT Steering Committee. The Administrator should establish a process to periodically review and refine the outsourcing contracts.

e) The Administrator should ensure that outsourcing of IT services or facilities does not weaken or degrade the Administrator′s internal controls.

f) The Administrator should ensure data security of sensitive information by putting in place the following (but not limited to) measures to ensure such as customer information:

i. Requiring the service provider to set high standards of due diligence and care in regard to security such setting security policies and procedures and implementing appropriate controls.

ii. Related staff of service provider should be granted access to information on “need to know” and “minimum authorization” basis;

iii. All outsourcing arrangements relating to policyholder information should be identified as material outsourcing arrangements;

iv. Strictly decide on and monitor any re-outsourcing actions of the service provider, and implement adequate control measures to ensure information security of the Administrator;

v. Ensure all related sensitive information be refunded or deleted from the service provider's storage when terminating the outsourcing arrangement.

2.4 Acquisition, development and implementation of information systems

a) The Administrator should have the capability to identify, plan, acquire, develop, test, deploy, maintain, upgrade, and retire information systems.

b) The Administrator's Board should ensure that acquisition or development of a new information system will support and enable the Administrator's strategy.

c) The Administrator should have policies and procedures in place to govern the initiation, priotisation, approval and control of information systems projects.

d) The Administrator should identify, assess and classify risks associated with IT projects. The risks should include operational risk, financial loss(es), and opportunity costs stemming from ineffective project planning or inadequate project management controls of the Administrator.

e) The Administrator should have a project management framework which should include the following:

   i. A clear definition of roles and responsibilities of project team members

   ii. Risk profiling – risk assessment and classification

   iii. Critical success factors for each phase of the project

f) The Administrator should document clear project plans for all IT projects that it undertakes.

g) The Administrator should specify functional and non-functional requirements for an information system including:

   i. security requirements
   ii. system access control
   iii. transaction authorisation
   iv. data integrity
   v. audit logs/trails
   vi. exception handling

h) The Administrator should adopt and implement a systematic system development methodology to control the life cycle of every information system. The system development methodology should be commensurate with the size, nature, and complexity of the IT project, and should generally facilitate the management of related risks. Phases should include system analysis, design, development or acquisition, testing, trial run, deployment, maintenance, and retirement.

i) The Administrator should establish a methodology for system testing that should include business logic, security controls and system performance.

j) The Administrator should maintain separate environment for system testing (including user acceptance testing) and system integration.

k) There should be restricted access to production site for members of staff.

l) The Administrator should set policies and procedures to control the process of system upgrade(s).

m) The Administrator should establish an effective problem management process in order to ensure that information system problems can be tracked, analyzed, and resolved in a systematic manner.

2.5 Business Continuity Management

a) An Administrator's board of directors and senior management should have oversight over business continuity management;

b) The Administrator should establish a Business Continuity Plan (BCP) on an enterprise-wide basis.

c) The Administrator should have in place appropriate arrangements in relation to the BCP/DRP, taking into consideration the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption.

d) The Administrator should regularly update and test the above mentioned arrangements to ensure their validity and effectiveness.

e) The BCP should include, but not limited to, the following:

   i. Business Impact Analysis (BIA);
   ii. Risk assessment, monitoring and testing;
   iii. Security standards;
   iv. Project management;
   v. Change control policies;
   vi. Data synchronisation procedures;
   vii. Crises management;
   viii. Incidence response;
   ix. Remote access policies and standards;
   x. Disaster recovery procedures;
   xi. Employee training and awareness;
   xii. Notification or communication standards and contact information;
   xiii. Insurance coverage.

f) In developing a BCP, an Administrator should consider the likelihood and impact of a disruption to the continuity of its operation from unexpected events.

g) The Administrator should assess the disruptions to which it is particularly susceptible including but not limited to:

   i. loss of failure of internal and external resources (such as people, systems and other assets);

   ii. loss or corruption of its information; and

   iii. external events (such as war, civil strikes, fire etc.).

h) The Administrator should consider categorising disruptions into short-term, medium term and long-term disruptions and make appropriate arrangements to reduce the impact of any occurrence of the disruptions. Such arrangements should include:

   i. Resource requirements e.g. people, systems and other assets,

   ii. arrangements for obtaining these resources;

   iii. The recovery priorities for the Administrator's operations; and

   iv. Communication arrangements for internal and external concerned parties (including RBM, clients and the press);

NOVEMBER 2014

PENSION AND INSURANCE SUPERVISION DEPARTMENT