Internal Audit Control Measures from a Risk Management Perspective

Closed Pension Fund Administrators

A MILLIMAN GLOBAL FIRM
H R Nigeria Limited
Consultants and Actuaries

8th Floor, Aiico Plaza, Afribank Street
Victoria Island, Lagos
Tel\Fax: 2610708, 4616768, 4616859, 4627313-4
info@hractuaries.com
www.hractuaries.com

May 2007

Table of Contents

INTERNAL AUDIT CONTROL MEASURES
FROM A RISK MANAGEMENT PERSPECTIVE - CPFA

1. INTRODUCTION

This document is prepared to discuss audit control measures from a risk management perspective.

2. RISK IDENTIFICATION

We have identified, and briefly discuss the 12 risks faced by the CPFA enterprise.

S/N	RISK TYPE
1	Liquidity Risk
2	Interest Rate Risk
3	Credit/Deposit Concentration Risk
4	Market Risk
5	HR Risk
6	Health and Safety Risk
7	Infrastructure Risk
8	Information Systems Risk
9	Fraud risk
10	Security Risk
11	Legal Risk
12	Operational Risk

2.1 Types of Risks – Strategies for managing them.

S/N	RISK TYPE	MITIGATION STRATEGIES
1	Liquidity Risk	• Routinely project Funds income/outgo profile at least quarterly in advance • Monitor tenure of deposits
2	Interest Rate Risk	• Market intelligence on liquidity flows and interest rate movements • Market intelligence on national political state • Weekly simulation of positions under different interest rates scenarios • Investigation of tenor – bond/market instruments • **Track** movements in market interest rates as well as reasons for the movements.
3	Credit/Deposit Concentration Risk	• Use Risk Acceptance Criteria before making investment • Apply sectoral and single obligor limits for Corporate bonds • Adopt risk rating agencies • Acquire market intelligence on financial status of banks, companies sponsoring bonds • Constantly monitor and report on the portfolio performance
4	Market Risk	• Have a well-documented Investment strategy, understood by Investment Team members. • Adhere to specified investment limits set by Investment and Risk Committees. • Continuously monitor trading positions • Market intelligence on political 'state'
5	HR Risk	• Have a good appraisal system that aligns company with individual goals • Constant training and retraining of new and existing members of staff • Ensure that every job function can be performed by at least two people. • Create opportunities for staff to be redeployed to sponsoring company. • Hold regular staff meetings
6	Health and Safety Risk	• Installation of internal alarm system • Training of staff on fire drills and use of fire extinguishers • Subjection of all staff to pre-employment medical examination. • Adequate maintenance of fire extinguishers and smoke detectors • Regular maintenance of vehicles.

7	Information Systems Risk	• Installation of anti-virus software. Check for License validity. • Acquisition of power backup system - Generator, inverters, etc • Installation of smoke detectors, sprinklers, and fire extinguishers in the computer room • Enforcement of hardware and software securities. These include locking of computers, and use of access rights and passwords to protect files and systems. • Restriction of physical access to the computer room through locks and prohibition of entry by unauthorized personnel. • Establishment of offsite backup office • Establishment of an effective disaster recovery plan • Constant fumigation of the office to remove rodents • Stabilisers, UPS, AC's, to be switched off at the end of the day. • Continuous training of staff both technical and non-technical to acquaint them with adequate knowledge required to do their jobs. • Payment of good compensation package and provision of good work environment to discourage IT staff from leaving the company to seek same outside. • Cover all computer equipment in a comprehensive computer insurance policy • Adequate maintenance of all the hardware and software equipment through maintenance agreements with the vendors.
8	Fraud risk	• Segregation of duties • Regular Reconciliation of Accounts • Good accounting system/controls • Authorisation control • Well defined policies and procedures • Good recruitment process - references, personality tests • Good compensation package • Log of activities • Fidelity guarantee insurance
9	Security Risk	• Adherence to laid-down procedures on opening and closing of entrance doors. • Proper procedures for receiving visitors
10	Legal Risk	• Use of lawyers to vet every agreement • Proper documentation of transactions • Defining Service Level Agreements (SLA) • Good filing system
11	Operational Risk	• Interface with Custodian to ensure resolution of issues - Remittances, Portfolio issues and reconciliation. • Proper interface exist between units and SLA are defined.

3. AUDIT CONTROL STEPS

To assist audit, we highlight below sources of risk under Finance/Investment, Operations, and IT.

3.1 Investment

Risk Sources

NO	RISK TYPE	LIKELY SOURCES
1	Liquidity risk	• Mismatch of asset type to liability profile such that Fund income stream is insufficient to meet outgo. • Concentration of assets sources in a few organizations • Bond Issuer negative cash flow • Sudden inability of an obligor to meet a maturing obligation due to systemic problems or adverse monetary policies. • Over Investment in assets that are not liquid (e.g. property)
2	Credit Default Risk	• Downgrade in stock rating possibly due to previous misinformation • Political downturn • Inexperienced rating agency – who is/are rating agency?
3	Concentration Risk	• Concentration of assets in few Sectors or indeed companies • Failure to exercise due control over the asset generating units.
4	Interest rate risk	• Sudden political instability • Market Economic Intelligence • Unexpected sustained high inflation • Asset spread
5	HR Risks	• Dissatisfaction from members of staff due to inability to realize personal goals • Engagement of inexperienced hands in the unit. • Inability of the direct assistant or any other person in the unit to effectively take over from the unit head. • Limited scope for expansion leading to inability of staff growth. • Lack of manpower training and development • One-man department
6	Information Systems Risk	• System Breakdown • Under protection (virus, service agreement etc)
7	Legal Risks	• Improper documentation of transactions • Loss of documents • Bad contracts
8	Fraud Risks	• Weak controls.
9	Errors in executed investment transactions	• Failure to post transactions from source documents • Inadequate check before authorization of transactions.

Audit Control Steps

- Ensure that all investments go through the formal investment approval process and have met the company's Risk Asset Acceptance Criteria
- Ensure that necessary documents exist for investment activities
- Ensure that there is a daily review of outstanding positions and that this review is evidenced in writing.
- Portfolio reconciliation with Custodian
- Regular reconciliation of Investment with General Ledger
- Ensure there is availability of Market Intelligence e.g. subscription to Investment Houses that provide daily/weekly/quarterly information sheets.
- Ensure HR issues are addressed/monitored

3.2 Operations

Risk Sources

No	Risk Type	Likely Sources
1	Operational Risk	• Data entry error • Misfiling
2	HR Risk	• Dissatisfaction from members of staff due to inability to realize personal goals • Engagement of inexperienced hands in the unit. • Inability of the direct assistant or any other person in the unit to effectively take over from the unit head. • Limited scope for expansion leading to inability of staff growth. • Lack of manpower training and Development • One-man department
3	Information Systems Risk	• Inadequate knowledge of systems • Absence of defined system Administrator • Inadequate system support • Failure to follow laid-down procedures in the processing of transactions

Audit Control Steps

- Ensure that a thoroughly documented **Operational Manual** exists. This manual should identify processes and procedures and have flowcharts.
- Ensure that the filing system is consistent with the procedure on filing
- Ensure reconciliation of Contribution schedule sent by both Employer and Custodian.
- Ensure there is validation checks on data and alterations are not permissible unless authorised.

- There should be a service level agreement which includes interface between the operational software service provider and the operators
- Ensue that actual vendor Service delivery is being monitored against required Service Levels.
- Ensure that actions are taken to correct identified lapses in Service Levels.
- Ensure that there is a training plan for the unit (especially on IT) and that this plan is being followed.
- Ensure that the recruitment process is followed for every new member of staff.
- Ensure that departmental meetings are being held and that staff have the opportunity to express their opinions on the situation of things in the unit.
- Ensure that contingency plans are in place – systems, safety etc - and that staff in the unit have undergone training based on the contingency plan.

3.3 Information Technology

Risk Sources

No	Risk Type	Likely Sources
1	Information System Risks	▪ Virus Attack ▪ Lack of adequate power supply ▪ Spikes and surges ▪ Flooding resulting from leaking roof or unlocked tap ▪ Fire ▪ Malicious Hacking ▪ Theft ▪ Fraud ▪ Destruction of network backbones by rodents ▪ Sabotage by employees ▪ Errors and omissions on the part of users ▪ Lack of competence and skills
2	HR Risks	▪ Poaching of experienced hands ▪ Dissatisfaction from members of staff due to inability to realize personal goals ▪ Engagement of inexperienced hands in the unit. ▪ Inability of the direct assistant or any other person in the unit to effectively take over from the unit head. ▪ Limited scope for expansion leading to inability of staff to grow.
3	Liquidity Risk/Interest Rate Risks/Concentration Risks/Credit Default Risk	▪ Inability of the system to provide relevant data for monitoring these risks.
4	Legal Risks	▪ Bad contracts with suppliers and service providers ▪ Loss of Documents ▪ Improper filing
5	Regulatory Risks	▪ The inability of IT systems to cope with increased regulatory requirements.
6	Cost Efficiency Risk	▪ Acquisition of irrelevant but expensive IT infrastructure ▪ Absence of good negotiation skills in the acquisition of new IT infrastructure.

Audit Control Steps

- Ensure the Installation of anti-virus software to detect and prevent virus infections
- Ensure the acquisition of a power backup system e.g. Generator, Inverter to provide power in the event of complete power failure from PHCN
- Ensure the installation of smoke detectors, sprinklers, and fire extinguishers in the computer room
- Ensure the enforcement of hardware and software securities in all our systems. These include locking of computers, and use of access rights and passwords to protect files and systems.
- Ensure the restriction of physical access to the computer room through locks and prohibition of entry by unauthorized personnel
- Ensure the establishment of an effective and functional backup system for backup of the company's essential information and data.
- Ensure the establishment of offsite backup and that the offsite location is well maintained in accordance with established procedure
- Ensure the establishment of an effective disaster recovery plan and also that the plan is regularly tested.
- Ensure constant fumigation of the office to remove rodents
- Ensure that Stabilizers, UPS, AC's, are switched off at the end of the day.
- Ensure that adequate care and caution is exercised in the disposal of IT assets. **Document procedures for disposal of IT asset.**
- Ensure that there is a training plan in the unit and that the plan is being followed.
- Ensure continuous training of non-IT staff on IT systems in use in the company
- Ensure that all computer equipment have comprehensive computer insurance policies
- Ensure that all computer equipment are raised above the floor using equipment stand in order to reduce the possibility of flood disaster due to plumbing leakage
- Ensure that there is a fire-proof data safe to be purchased and installed for keeping daily backup tapes on-site. The fire proof safe should also store monthly tape backup and soft and hard copies of all operational procedures, in addition to storing original application diskettes / CD ROMs.
- Ensure that Backup Servers are provided and configured with the same configuration as the Application Server and the Database Server.
- Ensure that approved processes and procedures are followed in the acquisition of any IT equipment or software.
- Ensure that there is maintenance agreement with reputable vendors for maintenance of the company's major I.T. systems
- Ensure that I.T. staffs are provided with telephones which will make it possible for them to be reached in the event of their inability to report at their duty post.

- Ensure that there are up-to-date copies of all operating procedures and instructions and ensure that they are kept in the following places and by the following persons from which and from whom they can easily be accessed:
  - Safe
  - Managing Director
  - Head of I.T.
  - Computer room
- Ensure that departmental meetings are being held and that staff have the opportunity to express their opinions on the situation of things in the unit.
- Ensure that comments in the appraisals are followed up and duly resolved.

3.4 Financial Reporting

We have omitted financial reporting audit controls/procedures above in the belief that the sponsoring company's procedures will suffice.

…….
O. O. Okpaise *ASA, FIA*
Managing Consultant

A MILLIMAN GLOBAL FIRM
H R Nigeria Limited
Consultants and Actuaries
May 2007