Technical Guide
on
Review and Certification of
Investment Risk Management Systems and Processes of
Insurance Companies

Committee on Insurance and Pensions
The Institute of Chartered Accountants of India
New Delhi

CONTENTS

		Page
	Foreword	***4***
	Preface	***6***
1	Introduction	***8***
2	Investment Function of Insurer	***11***
3	Information System Security and Audit	***21***
4	Coverage and Methodology of Review	***30***
5	Suggested Format of Audit Report	***67***
	ANNEXURES	
	CHECKLISTS FOR COMPLIANCE AS PER THE REQUIREMENTS OF IRDA	
Annexure 'A' Click here to view	Issues to be addressed along with application in R2 to IRDA	***72***
Annexure 'B' Click here to view	Review of Standard Operating Procedure Covering Systems & Processes	***77***
Annexure 'C' Click here to view	Review of Information Technology (IT) Systems and Processes supporting Investment Operations.	***89***

	APPENDICES	
Appendix 'A'	Insurance Regulatory and Development Authority (Investment) Regulations, 2000 Part 1 – Click here to view Part 2 - Click here to view	
Appendix 'B' Click here to view	Circular No. INV/CIR/008/2008-09 dated 22.08.2008 issued by IRDA to Insurers	
Appendix 'C' Click here to view	Relevant Portions of the Circulars of IRDA on Investment Function of Insurance Companies	
Appendix 'D' Click here to view	Requirements at the R1 / R2 Stage of Registration of Insurance Companies	

FOREWORD

Insurance aims to protect the owner from financial losses that he suffers for the risks he has taken. Ever since the Insurance emerged as a business, the Governments, in view of its very strong societal links, have felt the need for its proper monitoring and regulating. Regulating the investment function in this industry has become crucial in the market-driven economy, as the money involved represents huge savings of the public. Moreover, what the public invest in insurance companies is out of their savings and not out of surplus, unlike in the case of deposits with banks.

In order to protect the interest of policyholders, to regulate, promote and ensure the orderly growth of the Insurance Industry, the Government set up the Insurance Regulatory and Development Authority (IRDA) in 2000. The IRDA, in order to develop the insurance sector allows investing in different investment avenues, by weighing the various risks associated to efficiently serve the policyholders and also ensure an orderly growth of insurance business. The audit of investment functions of insurance companies is a necessary effort to ensure appropriate compliance with the various rules and regulations in this regard.

I am happy to know that the Committee on Insurance and Pension of the Institute has brought out this Technical Guide on Review and Certification of Investment Risk Management Systems and Processes of Insurance Companies providing detailed guidance on the manner of the audit of the Insurance and risk management systems and processes of insurance companies in accordance with the recent directions of the IRDA.

I believe that the instant publication is a laudable effort and a necessary step in the right direction as it attempts to provide guidance on critical issues to the members of the Institute as well as the various stakeholders. I am confident that this Guide would be received well by the profession and the industry.

I would like to thank the Chairman IRDA and his dynamic team for reposing faith in the profession for carrying out the Certification of Investment Risk Management Systems and Processes of Insurance Companies. I would like to

complement the Committee on Insurance and Pension and its Chairman, CA. Pankaj Inderchand Jain and his team for doing a valuable work in bringing out this Technical Guide.

New Delhi
26th November, 2008

Ved Jain
President

Preface

Since privatization of the insurance sector, there has been considerable growth in the insurance industry leading to sharp increase in the quantum of monies available with insurance companies. As a result the management of Investments has assumed greater importance in the over all interest of all the stakeholders as well as the economy. The Insurance Regulatory and Development Authority (IRDA) has always been very proactive in bringing out the relevant regulations for better management, reporting and protection of the interest of various stakeholders. The emphasis laid by IRDA on the System and Procedures of insurers to manage the Investments is also very laudable.

The IRDA has recently amended the Insurance Regulatory and Development Authority (Investment) Regulations, 2000 by issuing a circular, directing all insurers to file a compliance certificate issued by a Chartered Accountant, certifying that the Investment Risk Management Systems and Processes are in place and are working effectively.

The Institute of Chartered Accountants of India (ICAI) has always been working very closely with IRDA and has always tried to complement the initiatives taken by them. In response to the aforesaid circular issued by IRDA recently, the ICAI deemed it fit to bring out this Technical Guide on Review and Certification of Investment Risk Management Systems and Processes of insurance companies, providing detailed guidance on the manner in which the compliance verification of the Investment Risk Management System is required to be carried out in accordance with the circular issued by IRDA.

I take this opportunity to thank IRDA for reposing confidence in the ICAI for providing technical support in helping its members carry out the responsibilities given to them by the IRDA.

I place on record my sincere gratitude to CA. S.N. Jayasimhan, Deputy Director (Investments), IRDA, Shri A.V.Rao, Deputy Director (Actuarial), IRDA, CA. Viraj Londhe, CA. Viren Mehta and Dr. Vishnu Kanhere for preparing the basic draft of this Guide. I am also thankful to other members and Special Invitees of the Expert Study Group on Investment Function of

Insurance Companies of the Committee on Insurance and Pension of the Institute for their valuable contribution in finalising the Guide. I am also happy to acknowledge the guidance provided by the various insurance companies, by way of comments, on the exposure draft of this Technical Guide.

I am thankful to the President of ICAI, CA. Ved Jain and other members and special invitees of the Committee for their valuable guidance and cooperation in bringing out this publication. I appreciate the efforts put in by the officials of Secretariat of the Committee on Insurance and Pension for their contribution in timely releasing this Technical Guide.

New Delhi
27th November, 2008

CA.Pankaj Inderchand Jain
Chairman,
Committee on Insurance and Pension

1

INTRODUCTION

Introduction

1.01 Insurance in India has come of age. Insurers have been operating in India for a very long time, but were run by one life insurance and four State owned Insurance Companies. In the post- liberalisation phase, private insurers have also come on to the scene. Since insurance is concerned with the protection of a citizen's life and /or properties as well as national wealth, ever since insurance emerged as a business, Governments, in view of its strong societal links, have felt the need for its proper monitoring and regulating it through proper and extensive legislation.

1.02 Under the Insurance Regulatory and Development Authority Act, 1999 (IRDA Act), in order to protect the interests of holders of insurance policies, the Government set up the Insurance Regulatory and Development Authority (IRDA), on 19th of April, 2000, to regulate, promote and ensure the orderly growth of the insurance industry and for matters connected therewith or incidental thereto and further to amend the Insurance Act, 1938, the Life Insurance Corporation Act, 1956 and the General Insurance Business (Nationalisation) Act, 1972.

1.03 Insurance business has always been truly global and international in scope. Recognizing this, regulators of different countries banded together to form the International Association of Insurance Supervisors (IAIS). India is among the more than one hundred members of IAIS. The broad principles of IAIS are meant to see that:

- There is recognition of the fact that insurance is an international subject;
- Insurance requires to be monitored properly to ensure its healthy growth; and
- There is a standards setting mechanism.

1.04 The International standards are mainly concentrated in the following areas:

- Control over registration of companies
- Management of business through fit and proper persons to be employed
- Pricing of products to be done on scientific lines
- Management of Investments and associated Risks
- Maintenance of required Solvency margin
- Proper settlement of claims of consumers.

1.05 Hence, world over, the focus is on controlling the above key factors through regulations. In India, IRDA has implemented such controls through the following key regulations:

- IRDA (Registration of Indian Insurance Companies) Regulations, 2000
- IRDA (Assets, Liabilities and Solvency Margin of Insurers) Regulations, 2000
- IRDA (Appointed Actuary) Regulations, 2000
- IRDA (Actuarial Report and Abstract) Regulations, 2000
- IRDA (Investment) Regulations, 2000
- IRDA (Preparation of Financial Statements and Auditor's Report of Insurance Companies) Regulations, 2000
- IRDA (General Insurers – Re-insurance) Regulations, 2000

- IRDA (Life Insurers – Re-insurance) Regulations, 2000
- IRDA (Protection of Policyholders' Interest) Regulations, 2000
- IRDA (Distribution of Surplus) Regulations, 2000

2

INVESTMENT FUNCTION OF INSURER

Introduction

2.01 During the nationalized regime, state owned LIC and GIC along with its four subsidiaries were the only players in the country in life and general insurance business, prior to the advent of IRDA.

2.02 The investment portfolios of the insurance companies were earlier channelized to meet the objectives and priorities of the Government.

2.03 As per the recommendations of Malhotra Committee, the controlled investments in Government and approved securities of life insurance companies have been reduced to 50% while those for general insurance companies has been reduced to 30% of investible funds.

2.04 Thus a higher amount has been made available to insurers to invest in private and corporate sectors, housing and infrastructure sector, etc., to provide freedom in the structure of the investment portfolio but at the same time aligning it to fit into the overall investment strategy of the insurer. This required the regulators to frame regulations to make insurers properly use the freedom provided, but at the same time, through exposure norms, ensure such flexibility is not used beyond permitted levels .

2.05 Therefore, it would be proper to conclude that regulating the investment function in this industry is a necessity even in the market driven economy, as the money involved represents huge 'public savings'. Moreover, what the public invest in insurance companies is out of their

savings and not out of surplus, unlike in case of deposits with banks. It is because of this reason that the regulations keep 'policyholder protection' as its prime concern. But the regulator responsible for develop t he insurance sector allows investing in different investment avenues, by weighing the various risks associated to efficiently serve the policyholders and also ensure an orderly growth of Insurance business. The Audit of investment functions of insurance companies is a necessary effort in this direction.

2.06 Any insurance contract, ultimately, is based on fact as well as faith : Faith of the policyholders that if and when there is a claim under their policy it would be settled properly; that there are mechanism to ensure that the insurance company will be solvent for a period longer than the term of the policy.

2.07 By themselves, insurance companies are major players in a nation's economy. The sheer volume of monies itself speaks i ts role in the economy of India. In the financial year 200 7-08, for example, the Life Insurance Companies collected first year premium of Rs. 92988.71 crores, and Non-life Insurance Companies (including health insurers), collected a gross premium of Rs. 86242.13 crores making it to an aggregate of Rs. 1,79,230.84 crores.

2.08 The Non-life Insurance Companies hold 37.45% of their overall invested funds in Government securities (inclusive of state govt. and other approved securities), 7.43% in the Housing sector and 12.11% in infrastructure investments in 2006-2007 . The total invested funds (as of March 31, 200 7) were Rs. 50383 crores, which represented almost 19% increase in invested funds over the previous year. The national econo my has benefited significantly from this sector, since the rate of investment of these funds was considerably higher than the growth rate of the GDP.

2.09 Because of the quantum of monies that are involved and due to their significance, the channeling of insurance monies into proper sectors has assumed great importance and therefore the regulations, owing to national priority, have become crucial. So, IRDA would like to be very certain that these funds are properly invested as per the notified regulations, and that the investments are in line with national economic policy [which also takes into consideration the expectations of the policyholders].

Trade off in Investment Decisions

2.10 Though insurance companies provide solutions to risks of others, they have their own risk, both operational and financial. Investments always come with risk. However, the degree of risk varies based on the types of investments, quantum of money invested [exposure] and the term.

2.11 The Insurance company has to make a careful analysis before making any investment decisions, taking into consideration the nature of business, risk involved, return required to meet the actuarial assumptions on returns anticipated out of the investment to be made at the time of designing the product, liquidity requirements, regulatory prescriptions etc, .

2.12 Further, the investments made should also take into consideration the Policyholders' Reasonable Expectations (PRE) which has a bearing on the following factors:

- Guarantees made,
- Achieving a real return, that should be in excess of guarantees made, particularly on without profit policies,
- Realised returns are fairly consistent with returns of earlier period(s)

2.13 Objectives of regulating the Investments of the Insurance Companies

- The regulations aim to ensure the safety of funds, which belong to the policyholders.

- To maintain quality of invested assets to support the prescribed solvency parameters of the insurer.

- The occasional lower interest rate regimes could compel companies to seek alternate investment channels which would optimize the returns, but in such process would subject the investment to higher risks. Regulations would not allow exposure to such high risk investments.

- The prudential norms ensure proper spread and thus avoid 'concentration risk'. Hence investment regulations limit exposure to a particular company or a group (including group to which the insurer belongs) of companies or to a particular industry sector except Infrastructure to ensure proper diversification of the investment portfolio.

- Regulations also prevent an insurer from taking a controlling stake, out of policyholders' funds, in any company by limiting exposure either to 'Debt' or 'Equity' mode.

2.14. Another important factor in regulation of investment that cannot be lost sight of is the need to earmark some portion of investible funds for social obligations. The savings of the people coming to insurance companies by way of premium have to be channelized into community development, infrastructure development, socially oriented investments, provision for basic

amenities in rural areas etc. Towards this, IRDA (Investment) Regulations, 2000, provides for a mandatory minimum of 15% and 10% of Investible funds to be invested in Infrastructure in the case of Life and General Insurance Business respectively.

During the nationalized regime, state owned LIC and GIC along with its four subsidiaries were the only players in the country in life and general insurance business, prior to the advent of IRDA.

2.15 The investment portfolios of the insurance companies were earlier channelized to meet the objectives and priorities of the Government.

2.16 As per the recommendations of Malhotra Committee, the controlled investments in Government and approved securities of life insurance companies have been reduced to 50% while those for general insurance companies has been reduced to 30% of investible funds.

2.17 Thus a higher amount has been made available to insurers to invest in private and corporate sectors, housing and infrastructure sector, etc., to provide freedom in the structure of the investment portfolio but at the same time aligning it to fit into the overall investment strategy of the insurer. This required the regulators to frame regulations to make insurers properly use the freedom provided, but at the same time, through exposure norms, ensure such flexibility is not used beyond permitted levels.

2.18 Therefore, it would be proper to conclude that regulating the investment function in this industry is a necessity even in the market driven economy, as the money involved represents huge 'public savings'. Moreover, what the public invest in insurance companies is out of their savings and not out of surplus, unlike in case of deposits with banks. It is

because of this reason that the regulations keep 'policyholder protection' as its prime concern. But the regulator responsible for develop the insurance sector allows investing in different investment avenues, by weighing the various risks associated to efficiently serve the policyholders and also ensure an orderly growth of Insurance business. The Audit of investment functions of insurance companies is a necessary effort in this direction.

Investment Function of Insurer - Regulatory Framework

2.19 The Insurance Act, IRDA Act and the Regulations made there under which are relevant for the inspection of investment function of Insurance Companies are featured with some technical terms/concepts whose familiarization is critical for the inspector to perform his function. There are references to some other statutes such as Public Debt Act, 1944, Securities Contract Regulation Act, 1956, etc in the above-referred regulations. This chapter lists all the relevant provisions of the related statutes (regarding those technical terms/concepts) at one place so that it will be like ready reference to the members involved in this exercise.

2.20 The primary legislations, which are relevant for investments of insurance companies in India, are as follows:

- Insurance Act, 1938;
- Insurance Rules, 1939;
- Insurance Regulatory and Development Authority Act, 1999;
- Insurance Regulatory and Development Authority Regulations issued under IRDA Act, 1999 from time to time;
- Insurance Regulatory and Development Authority (Investment) Regulations, 2000 as amended from time to time;
- Insurance Regulatory and Development Authority (Preparation of Financial Statements etc.) Regulations, 2002;

- Insurance Regulatory and Development Authority (Assets, Liabilities and Solvency Margin of Insurance Companies) Regulations, 2000 and
- Circular(s) issued by IRDA on Investment Function and amended from time to time.

IRDA (Investment) (Fourth Amendment) Regulations, 2008

2.21 A Working Group was set up by the IRDA, to evaluate comprehensively the regulatory and other provisions on Investments of Insurance companies and propose changes considered essential in the light of experience gained and / or the difficulties faced by Insurance Companies in complying with the various legal and regulatory requirements , as well as the developments in Financial Markets including the emergence of Unit Linked Insurance Policies as one of the most important product portfolios of life insurers.

2.22. Accordingly, the Working Group reviewed the statutory provisions on the pattern of Investment, operational and policy issues of Investment Regulations, and suggested amendments that would give flexibility to the IRDA with reference to the Regulation on Investment of Life and General Insurance Companies. Apparently the Group also looked into the concurrent modifications in the formats of the prescribed Returns to reflect the changes as reflected in the revised formats under the IRDA (Investment) Regulations, 2000.

2.23 The recommendations of the Working Group were examined by IRDA in the light of legal provisions, keeping in view the interests of the stakeholders.

2.24 Accordingly, the Authority amended the provisions of IRDA Investment

Regulations 2000 in order to implement the recommendations of the Working Group and also to effect such changes that are considered necessary to clarify the existing regulatory requirements. The IRDA Investment Regulations 2000 as amended by the Insurance Regulatory and Development Authority (Investment) (Fourth Amendment) Regulations, 2008 is given in Appendix 1 to this Technical Guide.

2.25 IRDA has also decided to effect some modifications in the extant Guidelines / Circulars on investment portfolio [Annexure - II to Circular INV/CIR/008/2008-09 dated 22.08.2008 issued by IRDA to Insurers – the said circular has been given as Appendix B to this Technical Guide] and also introduced certain requirement on the Systems / Process of investment in the context of Risk Management requirements. The proposals of IRDA in this regard have been outlined in Annexure – III to Circular INV/CIR/008/2008-09 dated 22.08.2008 issued by IRDA to Insurers (Appendix B to this Technical Guide). This Technical Guide is specifically meant for review and certification of Investment risk and management systems of Insurance companies arising out of the IRDA (Investment) (Fourth Amendment) Regulations, 2008 and the circular No. INV/CIR/00 8/2008-09 Dated 22nd Aug, 2008 issued by the IRDA.

SCOPE AND COVERAGE OF THIS TECHNICAL GUIDE

2.26 While the first Chapter of this Technical Guide is intended to provide a general overview of the insurance sector in India, the second chapter has been structured to present the important issues related to the investment function of insurance companies. Third Chapter of this Guide deals with the role of information system security and audit in the investment risk management systems and processes of insura nce companies.

Fourth Chapter of this Technical Guide provides detailed guidance on the review and certification of the Systems / Processes of investment in the context of Risk Management requirements as contained in Annexure III of the aforesaid circular of the IRDA. Suggested Format of the Auditors Report after reviewing the Systems / Processes of investment of insurance companies in the context of Risk Management has been given in the Fifth Chapter.

2.27. Three Annexures to this Technical Guide contains three different checklists templates purposes of which are as under:

- Checklist template prepared to cover some key Regulatory issues that IRDA had in the past identified through periodical Investment Inspections has been given as **Annexure A**
- Checklist given in **Annexure B** contains the key issues to be addressed while reviewing the Standard Operating Procedures of existing insurance companies with regard to the investment Operations and risk management systems and processes envisaged by its guidelines Annexure II and III to the circular No. INV/CIR/008/2008-09 Dated 22nd Aug, 2008 issued by the IRDA.
- Checklist given in **Annexure C** covers the information technology related compliance on insurers as envisaged by Regulations 8 under FORM IRDA / R2 Application of Registration in IRDA (Registration of Indian Insurance Companies) Regulations, 2000 .

2.28 Insurance Regulatory and Development Authority (Investment) Regulations, 2000 as amended by Insurance Regulatory and Development Authority (Investment) (Fourth Amendment) Regulations, 2008, Circular No. INV/CIR/008/2008-09 dated 22.08.2008 issued by IRDA to Insurers and

relevant portions of the Circulars of IRDA on Investment Function of Insurance Companies have been given as **Appendices** to this Guide**.**

3

INFORMATION SYSTEM SECURITY AND AUDIT

INTRODUCTION

3.1 Information systems (IS) play a key role in the operations of a business organization. In fact information is the life blood of business and this is equally true of the Insurance sector. A proper framework that addresses governance, risk and compliance depends on the support of robust IS that ensure confidentiality, integrity and availability of information. Similarly , the IS facilities in turn need to be governed by appropriate policies, governed by best practices, guided by specific procedures and supported and manned by trained people. Information Security has assumed great importance due to the growing incidents and threats causing huge losses to business over the years, bringing about legislative and pro cedural changes in its wake.

3.2 The position of the Insurance sector is unique in as much as it has a dual role to play. One, that of protecting and securing its own information and infrastructure to realize its business objectives including managing it s investments for security, wealth / value maximization, solvency, liquidity and profitability, and the other, of promoting better information security through positive reinforcement and reward by providing insurance cover and lower premium for cyber risks of entities that have information security systems in place.

3.3. The increasing dependence of Insurance Companies on Information systems brings up issues – like data storage, retrieval, access and processing that is opaque and unintelligible to humans , loss of audit trail, adverse effect on controls – especially segregation of duties, and a lot more.

3.4.However, they also provide greater computing power that enables automation of processes and implementation of systems that streamline front, mid and back office operations, enable policy servicing, transparent accounting and customer communication and reporting, market information, valuation, NAV computation, and provide support for other compliance/regulatory requirements.

3.5. The important aspects and issues that necessitate inclusion of Information system controls, checks and balances for proper functioning of investment function and management of the risks are outlined below. These will set the tone for and provide proper perspective to the guide lines.

SECURING AND USING CUSTOMER INFORMATION AND DATA

3.6. Insurance business essentially deals with risk management and by its very nature is privy to sensitive information about customers. Information about their vulnerabilities and risks, their s hort comings and exposures ranging from business risks and exposures in loss of profits , policies relating to diseases, handicaps and family histories in case of health insurance.

3.7. It is not just the ethical and moral duty of the insurer to protect th e client data and store it securely but also a good business practice to secure it and share it only with authorized partners for permitted purposes.

3.08.In the years to come, as the Indian Insurance industry expands, goes global, and matures, the impact will bring about sweeping changes across the insurance Industry – in the way information is collected, stored, sent and accessed both internally and externally (4).

3.09. This will result in growth in staffing in the information security sector/segment, greater surveillance and monitoring mechanisms being put in place, and growing expenditure on information security. Insurance companies will have to start putting information security policies, procedures and best practices in place and will have to implemen t information security solutions and audit those at regular intervals.

3.10. This will also mean placing restrictions on indiscriminate access and use of customer data for cross-selling purposes, and also of selling customer lists and data bases for a pric e.

PREVENTING INSIDER ABUSE

3.11. Insurance companies by their very nature deal with a substantially large client base, their transactions span over a long time period (typically twenty plus years in the case of life policy), are open to abuse and misus e by unscrupulous clients and employees/agents (insurance frauds) and are also

exposed to management frauds through misrepresenting accounting estimates and window dressing.

3.12. The emergence of corporate governance and the responsibility of quick, timely and accurate reporting of information, now places an extra burden of maintaining confidentiality, integrity and availability of information on insurance companies.

PROTECTING DECENTRALIZED DATA

3.13. With the advent of networks, remote and tele-computing and spread of insurance services over geographical area, distributed data processing and multi-user computing has become the order of the day.

3.14. Data bases are no longer unified or centralized as in the past. Data is stored on different servers at different locations, needing broader security measures, which will ensure that protection levels are maintained across different networks and platforms.

MANAGING LEGACY SYSTEMS AND INTEGRATING SECURITY INFRASTRUCTURE

3.15. Insurers were one of the early users of data processing systems. Electronic Data Processing (EDP) has today grown into Information Technology (IT), but most insurance companies are still flogging the earlier legacy systems and programs which can be seen being used with the latest technology. Given this diversity of systems, using different operating platforms, different network architectures, different types and differing versions of software, ensuring compatibility of security tools and integration of security infrastructure has become a Herculean task, not to mention the

challenge of maintaining and ensuring effective and efficient functionality of the entire process.

INTERNET/WEB ACCESS TO DATA BASES AND APPLICATIONS

3.16. Most insurance companies, in an attempt to reach a larger number of customers and providing better service and lower cost , are web-enabling their businesses especially the delivery systems and interfaces. This has brought the security issues associated with the internet – especially unauthorized access, data modification and analysis, spoofing, passing off, identity theft, denial of service and hacking attacks, web vandalism, mistrust, privacy loss and repudiation – into sharp focus.

BALANCING SECURITY AND OPENNESS

3.17. Insurance requires an open environment where customers and agents get maximum access to the required data in an easy convenient way. Security features, which restrict or affect accessibility and ease of use, are bound to turn away customers from the most secure insurance company sites and portals. This is perhaps the biggest quandary in which insurers find themselves today. Ease of use, user-friendly interface and efficiency and innovation leading to fast processing speed and better customer service cannot be compromised by information security applications.

KEY ISSUES IN INSURANCE SECTOR

3.18.The key issues for information security in the insurance sector today, apart from putting in place necessary Investment Risk Management Systems and Process, are maintaining privacy and confidentiality of customer information and data, providing authenticity and integrity of data and transactions, identification of users, non repudiation and preventing

unauthorized access, insider abuse and cyber attacks and threats. It also revolves around ensuring efficiency and effectiveness of information systems and ensuring compliance with laws and building reliable systems.

THE ROLE OF IS AUDIT IN INSURANCE SECTOR

3.19. Information System Audit has a significant role to play in the emerging Insurance Sector. Information Syste m Audit aims at providing assurance in respect of Confidentiality, Availability and Integrity for Information systems. It also looks at their efficiency, effectiveness and responsiveness. It focuses on compliance with laws and regulations.

3.20. In the context of the growing dependence of Insurance Sector on Information Systems for record keeping, transacting business, reporting, as well as regulatory compliance and providing information and results to stakeholders, Information System Audit has assumed a ve ry significant role. In fact it would not be wrong to say that without effective IS Audit systems being put in place, corporate governance, compliance and effective regulation and risk management of the insurance sector would be a difficult proposition.

THE SOLUTION – A PROACTIVE APPROACH

3.21. It is always wise to put in place a proactive approach to security that is based on education, awareness exchange of information, policies, practices, procedures, cooperation and motivation of all concerned that will enable insurers to meet the information security challenges faced, as there will be no wastage of time to take control of adverse situation in the long run. Towards this, in protecting the huge Investments of Insurers, IRDA has

recently issued clear guide lines on Investment Risk Management Systems and Process.

THE SCOPE

3.22. With a view to addressing the concerns of the Regulator and other stakeholders, the audit for review of investment risk and management system should include within its scope the follo wing minimum areas of information system security and audit:

i. **Risk Management**: Ensure that the features and system parameters implemented in the system are in accordance with the policies and procedures covered in IRDA Investment Regulations and applicable Guidelines / Circulars.

ii. **Application Review**: Review and validate that the software used by the insurance companies is in accordance with the security standards and policies and guidelines as prescribed by IRDA.

iii. **Security Policy and Implementation**: Review the security policy and implementation procedures with special reference to the Hardware Platform, Network, Operating System, Physical Perimeter, Backups and databases.

iv. **Capacity Management**: Assess the existing and planned capacity for growth and adequacy of the current capacity to handle existing and future business.

v. **Disaster Recovery, Back-up and Contingency Planning**: Review of the existing disaster recovery, bac-kup and contingency plans and policies of the insurance companies and verify and assess the compliance to current policies.

vi. **Customer Services**: Review the procedures for providing services and communicating with clients / investors.

vii. **Internal Vulnerability Assessment**: Ascertain the data integrity, availability and security of the key information present in the network and the efficiency, effectiveness, responsiveness and compliance of the IS processing facilities.

THE APPROACH

3.23. The approach, Checklist based audit, should address and cover the following key activities of an Insurance Company:

i. Understanding the Information Technology Infrastructure of the insurance company as it exists at the location.

ii. Understanding the business process, related to the Investment function and risk management system.

iii. Understanding the transaction mechanism and data flow with respect to investment management function.

iv. Inspection and review of the documented policies and procedures, infrastructure and network diagram.

v. Collection of evidence in the form of documents, test results, screenshots, confirmations, logs, third party evidence.

vi. Conducting a risk analysis in the environment to evaluate and test the existing risk management processes and available controls, both system- based and manual.

vii. Vulnerability analysis and - audit of host servers.

viii. Discussing critical observations / findings with the Insurance Company and generating a report to be submitted to IRDA.

4

COVERAGE AND METHODOLOGY OF REVIEW

INTRODUCTION

4.1 Insurance Regulatory and Development Authority of India **(IRDA)** has amended the Investment Regulations vide notification dated July 30, 2008 and issued IRDA (Investment) (Fourth Amendment) Regulations, 2008. Further, vide circular no. INV/CIR/008/2008-09 dated August 22, 2008 IRDA has introduced specific minimum requirements on the Systems / Process of investment in the context of Risk Management viz. Investment Risk Management Systems**.**

4.2. All Insurance Companies seeking registration with IRDA on or after August 22, 2008 need to comply with Investment Risk Management Systems and Processes as a part of registration process. All existing Life and General Insurance Companies have been required to obtain a certificate from a Chartered Accountant's firm — that it is not the Statutory or Internal or Concurrent Auditor of the concerned Insurer and has a minimum of three to four years of' audit experience of IT systems, risk management and process controls of Banks or Mutual Funds or Insurance Companies — to the effect that Investment Risk Management Systems and Processes envisaged in Annexure III of the aforesaid circular are in place and working effectively. Further the Chartered Accountant's certificate needs to be filed with IRDA not later than the first week of January 2009.

4.3 GENERAL

4.3.1. FRONT & BACK OFFICE OPERATIONS:

Investment Management System (IMS) *has following generic modules:*

- *Front Office*
- *MID Office*
- *Back Office*

BRIEF FEATURES OF IMS MODULES

Front Office module (FOS)

FOS is further divided into ***Fund Manager*** *module and* ***Dealer module****. Generic features of FOS are:*

It facilitates authorization of deals, order placement and entry of executed deals. It provides analytical tools, facilitates monitoring of investment restrictions, exposure limits and has risk management tools. The cash and securities position can be uploaded in the FOS to facilitate adherence to internal and regulatory limits.

MID Office module (MOS)

All ***investment deals*** *flow from FOS to MOS.* ***Risk Analysis, risk measurement and Risk Management*** *are a function of MID Office. Various risk measurement and management tools are applied to the trades and portfolio in the mid office module. These risk measurement functions are*

sometimes made part of FOS. However, in banking industry, Risk Analysis and Management function is entrusted to mid office team with the help of MOS.

Back Office Module (BOS)

All investment deals flow to BOS from MOS, where the same are ***settled****. In case of equity securities, deals forwarded by dealer are matched with the data of executed deals received from the brokers through Straight Through Process(STP) gate in BOS and confirmation is sent to broker and custodian. In case of debt securities, BOS generates the Counter party confirmation and custody letter for settlement of deals. The deals are pushed for accounting in the form of deal summary or trade blotter from the BOS to Fund Accounting System.*

An Auditor entrusted with the responsibility of certification of Investment Risk and Management System or otherwise is expected to gather good understanding of the IMS used by the insurer as this is the backbone of the investment department of Insurer.

a. Insurer having Assets under Management (AUM) in excess of Rs.500 Crores shall ensure separate personnel acting as fund manager and dealer

This clause requires the auditor to ensure that the insurer having asset under management ***(both Shareholders' and Policyholders' investment taken together)*** in excess of Rs. 500 Crores has separate Fund Managers and Dealers, for both Equity and Debt portfolio.

The auditor has to confirm that:

- There are separate Fund Managers and dealers for equity as well as debt segment by reviewing the organization chart of the company.

- Functional responsibilities of Fund Managers and dealers are defined in the Standard Operating Process (SOP) /Operations Manual or Investment Policy.

The auditor should review sample deals, either in software system or hard copies to confirm that all the deals are authorized by Fund Manager and executed by Dealer.

b. ***The Investment System should have separate modules for Front and Back Office.***

This clause requires the auditor to verify that the investment system has Front Office and Back Office Modules in the IMS.

The auditor should review the software system to confirm that it has separate modules for dealing and settlement. The auditor should **confirm** that these activities are carried out **by separate officials** with separate logins and passwords. The auditor can confirm this aspect through review of system and observing the process of trade execution and settlement.

c. ***Transfer of data from Front Office to Back Office should be electronic without Manual intervention (Real time basis) i.e., without re-entering data at Back Office.***

This clause requires the auditor to verify that there is no manual intervention for transfer of data from Front Office/MID Office to Back Office.

The auditor should review the software system to confirm that deals **for all types of securities** captured and authorized in FOS, automatically flow to BOS.

The auditor can review this aspect by entering different types of investment transactions in FOS and confirm that there is seamless flow of deals from FOS to BOS and in turn from Front Office to Back Office.

d. ***The Insurer may have multiple Data Entry Systems, but all such Systems should be seamlessly integrated without manual intervention.***

This clause requires the auditor to report whether manual intervention is required for integration of data entered through multiple data entry systems.

In the case of integrated system, usually seamless integration between front office, mid office and back office would exist. The auditor can review this by carrying out the limited review of the system.

In case Front Office, MID Office and Back Office systems are separate, the auditor would have to **ascertain** that,

- These systems facilitate upload between systems with due authentication/validation process that has been duly approved by the Investment Committee of the Insurer.
- No double data entry is required at any point.

The auditor has to review the live operations of the investment department in real time to ascertain the integration of these systems and to verify the approval of the Investment Committee for such integration through upload of data from one system to another system.

e. ***The Front Office shall report through the Chief Investment Officer (CIO) to the Chief Executive Officer (CEO). The Mid Office and Back Office, to be headed by separate personnel, shall be under the overall responsibility of Chief Financial Officer (CFO) who shall independently report to the CEO.***

This clause requires the auditors to ascertain the separation of investment and settlement function.

The auditor should review the following aspects with particular attention to whether '**investment**', '**review '& Monitoring**' and '**settlement**' functions are clearly separated as per SOP as well as through 'internal reporting':

- Organization Chart
- SOPs / Operations Manual / Investment Policy to understand the roles of officials of Front office, Mid office and Back office, CEO, CFO and CIO
- Reporting lines

4.3.2. EMPLOYEE DEALING GUIDELINES

a. ***The Standard Operating Procedure (SOP) followed by the Insurer shall clearly specify the Guidelines to be adhered to by the Dealer, that is, the Insurer shall clearly specify the Trading guidelines for***

Personal Investments of the dealer. The compliance of this requirement shall be commented upon by the Internal / Concurrent Auditor.

This clause requires the auditors to comment on employee dealing policy of the Company and adherence to the guidelines laid down in this regard..

The auditor has to confirm that the company has framed Employee Dealing Policy for dealing in securities by:

- Fund Manager
- Dealer
- Research personnel &
- Head of all departments

who possess/are likely to possess insider information (termed as **'Key personnel')**.

The Auditor has to verify that the Employee Dealing Policy inter alia contains the following **minimum** criteria:

i. List of key personnel covered under the employee dealing policy;
ii. Type of Investments covered such as equity, derivatives, investments in IPO etc.;
iii. Type of investments which would not be covered by these guidelines;
iv. Prior approval for dealing in securities from Compliance Officer for any trade;

v. Validity period of the approval i.e. the period within which a deal needs to be carried out after approval. If the transaction does not take place within the validity period, new approval needs to be obtained.

vi. Intimation of investment to be filed with Compliance Officer within specified time, say, within 7 days along with the proof of investment;

vii. Holding period of securities i.e. securities purchased should not be sold for specified period, say, within 30 days of purchase;

viii. Cooling-off period i.e. the period for the key personnel mentioned above during which they are not allowed to purchase/sell a particular security post transaction by the insurer;

ix. Restriction on short sale or square-off of the trades during the day.

x. Obtaining declaration relating to no self-dealing and Front running from key personnel;

xi. Periodic disclosures of portfolios and transactions, say, quarterly;

xii. Record keeping by Compliance Officer;

xiii. Details of penalty or Disciplinary Action for non-adherence;

xiv. Exceptions to the guidelines;

xv. Reporting to Board of Directors

The auditor should review sample transactions to confirm that the Company complies with the policy.

The auditor should also confirm that the scope of the internal/concurrent audit covers this aspect and the internal / concurrent auditors have commented on the same in their internal / concurrent audit report. This could be checked from engagement letter for the internal / concurrent audit and the internal / concurrent auditors reports submitted.

4.3.3. MAKER/ CHECKER PROCESS

*a. **Insurer should have the procedure of Maker / Checker mapped in their Standard Operating Procedure / Operations Manual of Investment Operations. The Internal / Concurrent Auditor shall comment on such practice in his report.***

This clause requires the auditors to comment upon whether maker/checker process is covered in SOP / operations manual of investment operations and whether adherence of maker /checker system is commented on by the internal/concurrent auditor.

The auditor has to **confirm** that the insurer has **SOP / Operations Manuals** covering:

- Investment operations for ALL types of investments such as equity, derivatives, Government Securities, debt and money market instruments
- Cash Management/Treasury operations
- NAV computation, where NAV is computed in-house
- **Valuation** of investments, under both Traditional and ULIP funds
- Empanelment of brokers

Review needs to be carried on the basis of the manuals to ascertain the maker/ checker principles are **embedded**. The Auditor should verify whether SOPs/Manuals provide for maker/checker control for all the important functions (**particularly where manual intervention is required**).

The auditor should also look at the processes which need to be carried out manually or require manual intervention such as deal entry, uploading prices for valuation, creation of masters etc. and confirm that the system has in-built maker/checker controls for such processes that are clearly documented and audited periodically for changes recorded.

The auditor should review the scope of Internal/concurrent audit to ascertain the inclusion of verification of maker/ checker compliance. He should also go through the internal / concurrent audit reports to ascertain /concurrent comments on this aspect.

4.3.4. AUDIT TRAIL AT DATA ENTRY POINTS

a. The Audit trail should be available for all data entry points including at the Checker / Authorizer level

This clause requires the auditor to comment on the audit trail maintained in the system for various activities.

The auditor should review the FOS, MOS and BOS and confirm that the **system maintains** audit trail for data entry, authorization, cancellation and any subsequent modifications. Further, the auditor shall also ascertain that the system has separate logins for **each user** and maintains trail of every transaction w.r.t. login ID, date and time for each data entry, authorization and modifications.

To gather information, the auditor can interact with the system administrator and see the log maintained in the **back-end** of the system for deal entry, authorization, modification and the period for which this log is maintained.

The auditor may enter a few dummy deals for modification and cancellation to check whether the system maintains log of every activity.

4.3.5. BUSINESS CONTINUITY PROCESS

a. To ensure Business continuity, the Insurer should have a clear Off-site Back-up of Data in a City falling under a different Seismic Zone, either on his own or through a Service Provider. Further, the Insurer / service provider (if outsourced) is required to have the necessary infrastructure for Mission Critical Systems to address at least the following:

1. Calculation of daily NAV (Fund- wise)
2. Redemption processing

This clause requires the auditor to comment on the **adequacy** of Business Continuity Plan of the company.

The auditor has to cover the following aspects in his review:

1. Back-up procedure (BCP) / Disaster Recovery Policy/ Manual of the company to ascertain if it covers the details of:

i. Detailed back-up policy for various data bases of the Insurer
ii. Various scenarios in which Disaster Recovery site needs to be activated and actions to be taken in such cases
iii. Details of **crisis management team** and **Business Recovery team**, **roles and responsibilities** of team members

iv. Processes to be carried out in case of disaster including activation of call tree
v. Contact numbers of **ALL** service providers and people in the organization responsible for/expected to be involved in the business continuity plan
vi. Critical functions for **EACH DEPARTMENT**, resources required for the same, and processes to carry out these functions
vii. Disaster Recovery measures

2. To ascertain whether the Insurer has their own Disaster Recovery site or an arrangement with service provider for Disaster Recovery site, at a seismic zone other than the one where Investment department is located and from where all operations relating to investment, risk management, settlement, Cash Flow preparation, NAV computation, funding for redemption processing can be carried out. The auditor should visit BCP/DR site of the insurer and **ensure** that the site has the following features:

i. Front Office/Back Office **software**;
ii. Policy servicing software (***for ascertaining the units to be redeemed***)
iii. NAV computation **software**;
iv. Bloomberg/Reuters/Television for market information;
v. NDS/NDS OM;
vi. Bond Valuer or any other software used for valuation;
vii. STP gate;
viii. Mail Back-up;
ix. Back-up of server data to access the contact details of custody, counter parties, brokers etc.;
x. Telephones / fax machine / printer etc.;

xi. Soft and Hard copy of Standard Operating Procedures (SOP) available at the site

3. That the insurer has carried out BCP testing **at least** once in a year and has prepared BCP testing report. Verify the **adequacy of the coverage** and whether report was placed before the Audit committee and/or Board of Directors.

4. Review confirmation obtained by the insurer for successful testing of BCP/DRP from the custodian.

5. In case the insurer has outsourced NAV computation activity, report / confirmation on BCP/DRP testing having been obtained from Fund Accountant. The auditor should comment on whether such testing is satisfactory.

4.4. FRONT OFFICE

4.4.1. SEGREGATION OF FUND MANAGER / DEALER

a. Investment Department should have documented the segregation of Fund Managers and Dealers through Authority Matrix as a part of its 'Standard Operating Procedure'.

This clause requires the auditor to confirm that the functions of the Fund Manager and Dealer are separated and clearly defined.

The auditor has to verify that the insurer has investment policy/ SOP clearly defining the roles and functions of Fund Managers and Dealers.

The auditor should peruse the SOP /operations manuals pertaining to Investment operations covering **ALL** types of investments such as equity, derivatives, Government Securities, debt and money market instruments and confirm that SOPs clearly state the activities to be carried out by Dealer and Fund Manager.

b. The Insurer should have documented the Access Controls and Authorization process for Orders and Deal execution.

This clause requires the auditors to comment on Access control and authorization process in FOS.

The auditor has to undertake the following tasks to comment on this aspect:

- Review the data access and data security policy of the company to confirm that it covers access controls.
- Confirm that the Company has approved and updated data access policy which states the access controls for each login ID.
- Review the system to confirm access controls have been defined in the software system for each login such as view, write, modify and authorization rights are defined user wise.

c. The Dealing Room should have a Voice Recorder and procedure for maintaining the recorded conversation and their disposal including procedure like no mobile phone usage in dealing rooms and other best practices.

This clause requires the auditors to comment upon voice recording system in the investment operations of the company. The auditor has to undertake the following tasks to comment on this aspect:

- Confirm that the Company has a voice recorder in the dealing room and all the dealing room phone lines are connected to the voice recorder.
- Verify that voice recorder is in working condition and has been tested at regular intervals by IT team. That there exists a process to retrieve the recorded voice and listen to the conversation.
- Confirm that tapes/records on which conversations have been recorded are preserved in fireproof cabins.
- Confirm that either mobile jammer is installed in dealing room or mobile phones are not allowed in the dealing room.
- The Auditor should also confirm the above aspects by surprise visits to dealing room.

4.4.2.INVESTMENT IN INVESTEE / GROUP COMPANY / INDUSTRY SECTOR

a. System based checks should be in place for investments in an Investee Company, Group and Industry Sector. The system should signal when the Internal / Regulatory limits are nearly reached PRIOR to taking such exposure and making actual investment.

This clause requires the auditor to comment on in-built controls in FOS or MOS to monitor investment restrictions prescribed in the Insurer's Investment Policy and under IRDA (Investment) Regulations.

For this purpose the auditor will undertake the following tasks:

i. Review the system to check if investment limits have been set w.r.t. Investee company, Group, Industry sector, rating, other

investment etc. as prescribed under IRDA Regulations and internal limits adopted, if any, by the company.

ii. Verify whether a report could be generated from the system enlisting these limits.

iii. Check if soft limits can be set in the system or that the system sends out alerts on nearing the set limit.

iv. Confirm that the system gives alert or sends exception report to Compliance Officer/CIO on breach of soft limit[1] on real time basis.

v. Verify that the system does not accept trade which would exceed the hard limit i.e. regulatory limit.

- In case of internal limits, check these aspects by carrying out review of the system and also by *entering a few sample deals* in FOS to verify that the rules are in-built in the system and they cannot be breached.
- Review the exception reports generated, if any.

4.4.3. INTER- FUND TRANSFER

a. The System should handle Inter- Fund transfer as per Circular IRDA-FA-02-10-2003-04. The Investment Committee may fix the Cut- Off time as per Market practice, for such transfer within the fund. (The inter- fund transfer should be like any other Market deal and the same needs to be carried out during the Market hours only)

[1] Soft limits means limits set in the system which are more stringent than the actual limits to be adhered to.

This clause requires the auditor to assess system's capability for carrying out inter-fund transfers in accordance with the regulation.

IRDA Circular No. IRDA-FA-02-10-2003-04 states that:

a. Transfer from shareholder's fund to Policyholder's fund should be at cost or market price whichever is lower. Debt securities should be transferred at amortized cost.

b. Transfer between policyholders' funds:

- In case of non-linked business, inter-fund transfer is not allowed.
- In case of unit linked business, inter-fund transfer is allowed at market price of the investment.

c. In case of small sized funds i.e. where policyholders' funds are less than Rs. 50 crores, sale of security at market price is allowed from shareholders' funds to policyholders' funds (and not vice versa) subject to certain conditions stated in the circular.

The auditor should review whether the system is capable of **ensuring** adherence to the aforesaid restrictions on inter-fund transfer. He has also to verify whether the system can **prevent** processing of inter-fund trade if carried out beyond market hours set as per the nature of security. For this, the auditor has to understand and check the controls set in the system. The auditor can use dummy trades of inter-fund by which system controls could be confirmed.

4.5 MID OFFICE

4.5.1. MARKET RISK

a. The system should be capable of computing various portfolio returns

This clause requires the auditor to comment on system's capability in computing *risk- adjusted portfolio returns*

Various ratios are used to measure the risk associated with the portfolio and the return, such as Sharp ratio, Tenor ratio, Sortino ratio, Stress testing, Back testing. The auditor should verify whether MOS or FOS or any other software acquired by the company is capable of computing these ratios.

The auditor should verify whether the process of computing Portfolio return analysis, if any, has been stated in the SOP or Operations Manual.

b. Regular limits monitoring and Exception Reporting. Also reporting on movement of prices

This clause requires the auditor to comment on the process of monitoring regulatory limits and movement in prices. The auditor should

- Verify that FOS or MOS monitors all the Regulatory limits on Exposure and Rating. FOS/MOS would have list of regulatory limits set in it. The auditor can confirm the function of limit monitoring by entering the sample/dummy deals in the system for various types of securities.

- The auditor has to ensure that regulatory limits set in the system are hard limits which cannot be breached.
- He should confirm that the right to set and modify such limits **does not** rest with front office or back office officials (this authority should be with Compliance Officer / Risk Officer.)
- The auditor has to ascertain if the system generates exception reports for breach of limits prescribed in the system.
- He should also ascertain whether the system has the capability to monitor price movement of securities held in the portfolio and parameterized reporting of exceptional price movement and its impact on the overall portfolio values.

4.5.2. LIQUIDITY RISK

a. ***The Insurer should have a Cash Management System to provide the funds available for Investment considering the settlement obligations and subscription and redemption of units etc, to pre-empt any leveraged position or liquidity risk.***

This clause requires the auditors to comment on robustness of cash management system to pre-empt leveraged positions or liquidity risk.

Robust cash management system provides current and projected **fund-wise** cash flow, without manual intervention, which facilitates accurate deployment of funds. With the help of **integrated** cash management system, funds availability serves as additional precondition to comply within the FOS, before accepting any trade. To comment on the adherence to this requirement the Auditor

- should **ensure** that Cash Management System is **not** managed using Spread Sheets.

- needs to verify that there exists an efficient cash flow management system through software, which would provide the exact cash position to Fund Manager from time to time to avoid any leveraged position, illiquidity risk as well as idle cash balances.
- should verify on sample basis the bank balances and ensure that there are **NO** instances of idle bank balances as well as over-drawn_bank balances and cash management system is indeed implemented.
- should report the software / systems used for cash management.

b. The System should be validated not to accept any commitment beyond availability of funds.

This clause requires the auditor to comment on the capability of the system to prevent dealing beyond funds available.

The auditor should confirm that the FOS has 'in-built' controls for not allowing any trade beyond the available cash except in case of trades for settlement date other than T date. This aspect could be ascertained by review of the system and also through putting sample dummy deals in the system.

4.5.3. CREDIT RISK

a. The Investment System should capture Instrument Ratings to enable it to automatically generate FORM 2 (Statement of Downgraded Investments) through the System.

This clause requires the auditor to comment on whether Form 2 can be generated from IMS or any other software used by the insurer.

The auditor should understand the process of generating Form 2 and ascertain if it is generated using system support. The auditor should verify on sample basis that downgrade in the rating is properly reflected in the Form 2 prepared through system.

The auditor should also verify that the security master contains the mandatory field as rating of the security and that the insurer has put in place a system to review the investment ratings of the securities and make amendments to rating in security master, if there is a downgrade in the instrument rating.

b. The System should automatically monitor various Regulatory limits on Exposure & Rating

This clause requires the auditor to comment on the ability of the IMS to monitor adherence to regulatory limits on exposure and rating on a regular and ongoing basis.

The auditor should review the FOS or MOS to check if various exposure and rating wise investment limits set in the system are mapped with the actual exposure of the fund-wise portfolio on periodical basis (daily in the case of Unit linked portfolio), and a report is generated by the system.

To ascertain the System's capability, the auditor should verify the reports generated by the system in this regard; dummy deals may be entered to check the system's functionality.

c. ***The System should have the ability to track changes in ratings over a period and generate appropriate alerts, along with the ability to classify investment between Approved and Other Investments***

This clause requires the auditor to comment on the system/procedure at the insurer's for tracking the changes in the ratings of the security and classification of the investments.

The auditor should verify whether there is a system in place to ensure that instruments downgraded below the minimum rating requirement for classification under 'Approved Investment' category as per Investment Regulations, are listed under 'Other Instruments' Investment category. To this end, the Auditor should verify that:

- the Security master of FOS contains the mandatory field of rating and classification of security as approved and other investments. The System should not allow creation of master without entering these details.

- the insurer has a system to monitor the ratings of the security. For that, check if the insurer has any sort of arrangement to receive update on rating of the security. *It may be specifically noted that the credit Rating should always be security-wise and* ***NOT*** *issuer-wise*.

- the security-wise rating received can be uploaded in the securities master to pick-up the revised rating that would be ideal. Alternatively, check whether a particular official is assigned the job of tracking the changes in the rating of the securities in the portfolio and updating the security master which would update the

classification of securities accordingly. (The User rights assigned to the Officer updating the Security Master for rating changes should be specifically commented on by the Concurrent Auditor as to whether the same is properly documented and periodically audited).

Verify whether the system automatically changes the classification of the security on change of rating wherever necessary in accordance with the IRDA (Investment) Regulations. Also verify on such changes, whether exception report is generated by the system for the use of compliance officer/risk officer and chief of Investments.

Regarding system ability to classify investment in 'Approved' and 'Other investment', the auditor has to verify whether the system has the ability to classify the asset as approved or otherwise based on various parameters of classification prescribed under Regulations such as dividend track record, rating, secured, investment more than the limit prescribed.

Verify that the process followed by the company in monitoring of changes in the rating and classification of asset is properly covered in the SOPs of the Company.

d. The Insurer should conduct periodic credit reviews for all companies in the portfolio. The periodicity should be clearly mentioned in the Investment Policy.

This clause requires the auditors to comment on system/procedure of the insurer for carrying out periodic credit reviews of all the companies in the portfolio.

The auditor has to understand the process followed by the company for periodic credit review of the companies in whose debt securities, the insurer has made investments. The reviews are carried out by a separate team such as a research team. The auditor has to ascertain and comment on the adequacy of credit reviews carried out by the insurer during the last one year and of the system support, if any, available for such review.

The auditor should review the Investment Policy to ascertain the mandate given by the Investment Policy for credit rating along with the periodicity.

e. The Insurer is required to keep a track of movement of Securities between Approved and Other Investments Status, as a part of Audit trail, at individual security level

This clause requires the auditor to comment on the process of the insurer for tracking the change in the status of the securities from Approved to other investments and vice versa.

The auditor has to review the process followed by the company to track the change in the investment status of the investment. For this, review the change in the classification of asset made by the Company. Peruse the SOPs to understand the process specified by the Company for such monitoring and re-classification.

Ascertain audit trail i.e. date of change, reason for the change, that is maintained for any change in the asset classification ideally through the system. Review MIS reports prepared for re-classification of investment,

if any. The auditor should obtain a trail from the system or otherwise, for any such changes and **confirm** that audit trail of all such changes has been maintained at security level.

4.5.4. TRACKING OF REGULATORY LIMITS

a. The System should have key limits pre-set for ensuring compliance with all Regulatory requirements and should be supported by work-flow through the System (real time basis) for such approval, if Regulatory limit is close to be breached.

For Guidance on how to confirm the adherence by the Insurer to this requirement, please refer to guidelines given for clause No. 4.4.2.a and 4.5.3.b.

b. The System should have the capability of generating Exception reports for Audit by Internal / Concurrent Auditor

This clause requires the auditor to comment on the systems of the insurer to generate exception reports pertaining to investments.

Exception reports relating to investment function should, inter alia, include – Change in the rating of the debt security, change in the status of investment from approved to other investment or vice versa, non-receipt of interest or redemption amount, non-compliance of various prudential norms prescribed under IRDA (Investment) Regulations and various circulars and guidelines issued under the Regulation, non-compliance of various internal limits set by the insurer.

The auditor has to review capability of IMS in generating such exception reports. For ascertaining this aspect the auditor may feed dummy deals in the IMS.

4.5.5. REVIEW, MONITORING AND REPORTING

a. The System should automatically track and report all internal limit breaches. All such breaches should be audited by Internal / Concurrent Auditor.

This is similar to clause 4.5.4.b above. Further, the auditor is required to comment whether software system (IMS) could track and report independently internal limit breaches (i.e., without manual invention).

b. Implementation and Review of Asset & Liability Matching and other Investment Policy Guidelines

This clause requires the auditor to comment on the implementation and review of guidelines prescribed in the Investment Policy adopted by the insurer.

The auditor has to ascertain that the insurer has prepared an Investment Policy in accordance with the Regulation 9 of the IRDA (Investment) Regulations, and it has been approved by the Board of Directors.

Investment Policy prescribes various guidelines for conducting the investment operations including Asset Liability Management.

The auditor also needs to confirm that the insurer has:

a. A mechanism to address the Asset Liability Management
b. Reviewed implementation of Asset Liability Matching mentioned in the Investment Policy and the same has been presented to Board on periodic basis at a frequency of not later than six months.
c. Carried out corrective actions, if any, as directed by the Board of Directors (BoD).

4.6. BACK OFFICE

4.6.1. DATA INPUT ERROR

a. The system should be validated in such a way that the Deal can only be rejected by the Back Office and not edited

This clause requires the auditor to comment on the access rights defined in the system for deal entry and modification.

Once a deal is concluded by the front office it flows to back office for settlement. The creator of the trade is front office and the job of the back office is restricted to verification of trade and then settlement. In view of this, back office should not have access rights to modify the terms and if any discrepancy is noticed, ideally, the deal needs to be rejected and pushed back to front office.

The auditor will verify if access rights are defined for each user and back office officials have only view rights and not the edit rights for deal entry.

The auditor should verify this aspect through system review as well as by actually trying to modify the deal in the BOS.

4.6.2. SETTLEMENT RISK

a. The System should be validated to restrict Short Sales at the time of placing the order

This clause requires the auditor to ascertain that FOS has in-built controls to prohibit sale of securities not held in the portfolio.

The auditor should ascertain whether there is a process to receive the data from the custodian for saleable quantity and upload it in FOS. The auditor should confirm that FOS contains a restriction for sale of security beyond saleable quantity. The auditor should confirm the same by putting dummy deals in FOS.

4.6.3. COMPUTATION OF 'NAV'

a. The System should be capable of computing NAV and comparing it with the NAV computed by the Service provider, if it is outsourced.

This clause requires the auditor to comment on the capability of IMS or Fund Accounting System to compute NAV. The auditor is also required to comment on the process of verification of NAV in case NAV function is outsourced.

In case, NAV computation is carried out in-house, the auditor should confirm that the system computes the NAV for each fund and plan without any manual intervention. (***Manual uploads of valuation inputs received, if any, from the external sources should be considered as***

manual intervention). This could be verified by reviewing the process of NAV computation in its entirety.

In case NAV has been outsourced, the auditor has to verify that the Company has a system in place to verify the NAV computed by service provider with the use of analytical techniques. This could be checked by review of working notes prepared/maintained by the insurer for NAV verification.

b. The Insurer should maintain NAV history (Fund-wise) in his Public Domain from the Start of the Fund to Current Date

The auditor should visit the website of the insurer to ascertain if fund-wise and plan-wise data of daily NAV is available since the beginning on the website of the company and is easily accessible to the user.

c. 'NAV' error – Computation and Compensation

1. All expenses and incomes accrued up to the Valuation date shall be considered for computation of NAV. For this purpose, while major expenses like management fees and other periodic expenses should be accrued on a day- to- day basis, other minor expenses and income can be accrued on a weekly basis, provided the non-accrual does not affect the NAV calculations by more than 1%.

This clause requires the auditor to comment on the process of NAV computation, particularly with focus on accruing income and expenses on daily basis.

The auditor is required to

- Review SOP prepared for NAV computation and ascertain the appropriateness of the method prescribed for deal booking, valuation, corporate action*, interest accrual, amortization, unit capital accounting, expenses accrual etc. Verify on sample basis NAV computation for different funds to ascertain that correct method is followed for NAV computation.

In case NAV computation is outsourced, then the auditor has to examine the NAV computation process followed at service provider to ascertain its appropriateness.

The auditor has to verify that all major expenses are accrued on daily basis and other expenses at least on weekly basis only if non-accrual on daily basis does not impact NAV by 1% or more.

2. ***Any changes in Securities and in the number of Units should be recorded in the books not later than the first valuation date following the date of transaction. If this is not possible, the recording may be delayed up to a period of seven days following the date of the transaction. Provided that the non-recording does not affect the NAV calculations by more than 1%.***

This clause requires the auditor to comment on promptness in recording of investment and unit related transactions.

The auditor has to

* Such as Stock Splits, Dividend, Rights Issues, Buy Back, Bonus Issues etc.

- Verify that all the investment deals and unit capital related transactions are accounted on a daily basis. He should peruse the SOP to understand the process defined for recording of investment transactions and particularly for unit capital transactions.

- Understand the process of recording missed transactions if any and whether there exists a mechanism to ascertain the impact of such omission and corrective action taken on the same.

If the insurer's accounting process is such that the transactions are not recorded on the same day, then what is the impact of non recording of transactions on daily basis, on the NAV and the delay in accounting is not beyond seven days, needs to be ascertained and commented upon.

3. In case the NAV of a Plan differs by more than 1% due to non - recording of the transactions, or any other errors / mistakes, the investors or fund(s), as the case may be, shall be paid the difference in amount as follows:-

This clause requires the auditor to comment on the process of compensating the investor in case of a mistake in plan-wise NAV of more than 1%.

The auditor has to ascertain the instances of mistakes in NAV. This could be ascertained by –

- Reviewing Instances of revision in NAV post declaration;
- Reviewing MIS report if any prepared for mistakes in NAV computation;

- Review of audit committee meetings
- Review of internal / concurrent audit report
- Obtaining instances of mistakes in NAV from the service provider in case NAV computation is outsourced

The auditor has to verify the process followed by the Company for compensating the investors due to mistakes in NAV computation and to state whether the process is in line with the clauses given below. Also, to verify whether a log of NAV errors is maintained in the system, and internal / concurrent auditor has commented on these mistakes.

- If the investors are allotted units at a price higher than NAV or are given a price lower than NAV at the time of sale of their Units, they shall be paid the difference in amount by the plan.

- If the investors are charged lower NAV at the time of purchase of their units or are given higher NAV at the time of sale of their units, the Insurer shall pay the difference in amount to the Plan and shall be compensated from Shareholders' portfolio that does not support Solvency Margin.

- The Internal / Concurrent Auditor shall look into the above issues and specifically report on it and comment on the Systems in place to take care of such issues on an ongoing basis.

4.6.4. ERRORS DURING BROKER EXECUTION LEG

a. All Equity deals should be through STP gateway for all broker transactions

This clause requires the auditor to comment on whether all equity deals are settled by Straight Through Process (STP).

All mutual funds, financial institutions, banks, insurance companies tie up with the service provider for STP. All deals entered in FOS by dealer are matched with STP files received from the broker in the BOS. BOS matches the deals and generates the files to be sent to custodian for settlement. These files are sent to custodian without any manual intervention.

The auditor should confirm that deal matching and settlement take place through STP as stated above. This could be checked by actually reviewing the day-end process at investment department.

4.6.5. UPLOADING OF VALUATION PRICE FILES

a. System to have capability to upload Corporate Actions such as Stock Splits, Dividend, Rights Issue, Buy Back, Bonus issues etc., for computation of NAV / Portfolio valuation

This clause requires the auditor to comment on the capability of the Fund Accounting system to compute NAV with least manual intervention.

The auditor has to verify that Fund Accounting system supports upload of:

- Deals from BOS
- Corporation actions* data received from custodian

* Such as Stock Splits, Dividend, Right Issue, Buy back, Bonus Issues etc.

- Valuations received from Gilt Valuer, Bond Valuer, FIMDA, BSE/NSE etc.
- Units data received from Policy Admin System

The auditor should also confirm that Fund Accounting system computes interest, amortization, expenses etc. and there is **no manual intervention** needed.

The auditor has to review the whole process of NAV computation and confirm it.

4.6.6. RECONCILIATION

a. Fund-wise, in the case of Life Insurers, reconciliation with Investment Accounts, Bank, and Custodian records should be done on a day-to-day basis for all types of products. In the case of ULIP products, Unit reconciliation with Policy Admin. Systems should be ensured on a day- to- day basis.

This clause requires the auditor to comment on reconciliation process of the insurer.

The auditor must review the SOPs to understand the process and responsibilities specified for various reconciliations. They also have to review the process of **fund-wise, plan-wise** reconciliation on sample basis for:

- Securities balance as per the books of account with the custodian records
- Bank Accounts

- Units Capital reconciliation –

  - *Subscription reconciliation i.e. balances as per books of accounts, balance as per Policy Admin records, and funds received for subscription*

  - *Redemption reconciliation i.e. balance as per books of accounts, balance as per Policy Admin System, and funds paid for redemption*

  - *Switch reconciliation i.e. balance as per books of accounts, balance as per Policy Admin System, and funds transferred for switch*

and **specifically comment** on whether the above are done on a day-to-day basis.

b. In the case of General Insurer / Re-insurer, reconciliation with Investment Accounts, Bank and Custodian records should be done on a day-to-day basis.

The auditor has to review the process as explained in para 6 (a) except for unit capital reconciliation.

4.7. INTERNAL / CONCURRENT AUDIT

a. An Insurer having Assets under Management (AUM) of not more than Rs.1000 Crores shall conduct a Quarterly Internal Audit to cover both Transactions and related Systems. Insurers having AUM above

Rs.1000 Crores should appoint a Chartered Accountant firm for Concurrent Audit to have the transactions and related Systems audited.

b. The Audit Report shall clearly state the observation at transaction level and its impact, if any at System level. The Audit Report shall be based on Exception Reporting.

c. The Auditor shall clearly state that the Insurer had done the reconciliations as required under point 4.6.6.a and 4.6.6.b

d. Segregation of Shareholders & Policyholders' funds:

1. In the case of a Life Insurer, each individual fund, both falling under Shareholders' / Policyholders', under any class of business, has 'scrip' level investments to comply with the provisions of Section 11(1B) of Insurance Act, 1938

2. Furthermore, the Shareholders' funds beyond Solvency Margin, to which the pattern of Investment will not apply, shall have a separate custody account with identified scrips for both Life and General Insurance Companies.

e. The Insurer is required to place the Audit Report before the Audit Committee and implement all its recommendations.

f. The Insurer shall, along with Quarterly Investment Returns to be filed with the Authority, confirm in FORM 4, that the Internal / Concurrent Audit observations, up to the Quarter preceding the

Quarter to which the Returns are filed, were placed before the Audit Committee for its recommendations, and action taken.

Note: Points 4.3.5.a.1 and 4.6.3 are specific to ULIP Business.

The auditor has to report on the scope and coverage of the internal audit in line with the areas stated under this clause.

As IRDA has prescribed requirement of concurrent audit, beyond Rs. 1000 Crores of AUM (Shareholders' and Policyholders' funds taken together) for investment operations to be carried out by the independent chartered accountant, if the insurer has not appointed the concurrent auditor, then the auditor has to state the plan of action of the insurer.

5

SUGGESTED FORMAT OF AUDIT REPORT

To the Board of Directors of
[Insert name of the insurance company]

We have examined the compliance of conditions of investment risk management systems & processes of ***[Insert name of the insurance company]*** (the 'Company') as stipulated in Annexure III of IRDA Circular Ref. INV/CIR/008-2008-09 on IRDA (investment) (Fourth Amendment) Regulations, 2008 (the 'Circular') issued by the Insurance Regulatory and Development Authority ('IRDA'), as on ***[insert date]***.

The design and implementation of the investment risk management systems and processes in accordance with the Circular and compliance thereto is the responsibility of the Company's management. Our responsibility is to examine the procedures, and implementation thereof, adopted by the Company for ensuring compliance with the Circular and state our findings.

An examination of the Company's compliance with the Circular includes examining, on a test basis, evidence supporting the management's compliance with requirements of the Circular. We have examined the relevant records and information systems of the Company and have obtained all information, explanations and representations from the ***[Chief Investment Officer or equivalent]*** & ***[the Chief Executive Officer or equivalent]***, (taken on record by the Board of Directors) which to the best of our knowledge and belief were necessary for the purpose of our examination. *[Further our procedures covered all the areas listed in the recommended Audit Checklist (Annexure B/C/D - Enclosed duly signed by us under reference to this certificate) issued by the Institute of Chartered Accountants of India in this connection.]* Our examination was performed in accordance with the Guidance Note on Audit Reports and Certificates for Special Purposes issued by the Institute of Chartered Accountants of India ("ICAI"). We believe that our examination provides a reasonable basis for our certificate.

We have not performed an audit, the objective of which would be the expression of an opinion on the financial statements, specified elements, accounts or items thereof, for the purpose of this certificate. Accordingly, we do not express such opinion.

Based on our examination, in our opinion and to the best of our information and according to the explanations given to us, ***[subject to the following:***

1*……*
2*……..]*
We certify that the Company has complied with the conditions of investment risk management systems & processes as stipulated in the Circular.

The key areas of non-mitigated/residual risk resulting from deficient investment risk management systems and processes identified by us during our examination are given in Annexure A appended herewith.

This certificate is solely for the purpose of submission to the IRDA and is not to be used, referred to or distributed for any other purpose without our prior written consent.

[Name of the Chartered Accountant firm]
Chartered Accountants

[Name of the Chartered Accountant]
Partner
[ICAI membership number]

Place:
Date:

ANNEXURE A

(FORMING PART OF OUR AUDIT CERTIFICATE DATED __/__/____)

Insurance Company Name : _____
Date(s) of Audit : _____

SUMMARY

CATEGORY	**NO. OF OBSERVATIONS**
INVESTMENT OPERATIONS (IO)	
Very Serious Irregularities (VSI)	
Serious Irregularities (SI)	
Procedural Irregularities (PI)	
SUPPORT IT SYSTEMS (SIS)	
Very Serious Irregularities (VSI)	
Serious Irregularities (SI)	
Procedural Irregularities (PI)	

KEY FINDINGS

NO	OBSERVATION, RISK AND ROOT CAUSE	RECOMMENDATION	IO / SIS	VSI / SI / PI
1				
2				
3				
4				
5				

[Name of the Chartered Accountant firm]
Chartered Accountants

[Name of the Chartered Accountant]
Partner
[ICAI membership number]

Place:
Date:

ANNEXURE B/C/D

(FORMING PART OF OUR AUDIT CERTIFICATE DATED __/__/____)

Detailed report in the prescribed checklist format [given as **Annexure A/B/C (as the case may be)'of this Technical Guide.**