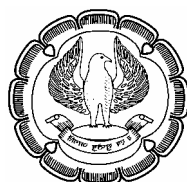


TRAINING MATERIAL ON INTERNAL AUDIT

DISCLAIMER:

The views expressed in this training material are those of the author(s) only. The Institute of Chartered Accountants of India may not necessarily subscribe to the views of the author(s).



The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

© The Institute of Chartered Accountants of India

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical photocopying, recording, or otherwise, without prior permission, in writing, from the publisher.

Edition : December, 2008

Price : Rs. 600/- (*including CD*)

ISBN : 978-81-8441-129-4

Email : cia@icai.org

Website : www.icai.org

Published by : The Publication Department on behalf of CA. Puja Wadhwa, Senior Assistant Director, Internal Audit Standards Board, The Institute of Chartered Accountants of India, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.

Printed by : Sahitya Bhawan Publications, Hospital Road, Agra 282 003.

December/2008/1000 Copies

FOREWORD

Internal audit helps the organizations to achieve their stated objectives. It does this by utilizing a systematic methodology for analyzing business processes, procedures and activities with the aim of highlighting organizational problems and recommending solutions. It is an important professional assignment being undertaken by members of the Institute both in practice as well as those in the industries. Every business entity needs their services as they provide valuable guidance in several aspects of running a business such as risk management, prioritizing goals, streamlining operations, device ways to cut operating costs, help the enterprise get maximum tax benefits, etc.

Carrying out an internal audit requires an in-depth understanding of the business culture, systems, and processes. To keep pace with change accelerates; internal auditors need to upgrade their existing knowledge and skill sets. I am pleased to note that the Internal Audit Standards Board is issuing Training Material on Internal Audit, containing extensive knowledge about the subject for use in their training programmes.

I congratulate CA. Abhijit Bandyopadhyay, Chairman, Internal Audit Standards Board and members of the Board on issuance of the Training Material.

I am sure that this Training Material would help the members and others who carry out the internal audit in understanding the concept and discharging their responsibility in an effective manner.

New Delhi

17th November, 2008

Ved Jain

President, ICAI

PREFACE

Organisations today operate in an economically, politically and socially charged environment. Further, the last fifteen years have seen novel business models being employed by the entities to sell their products and services. The decision making process for modern day organisations is, therefore, normally done in an environment which is constantly changing and fraught with a lot of uncertainty and risk. Even the slightest error in properly identifying and addressing risks can have a telling adverse impact on the future of an organisation. To strengthen their decision making process and to hedge against the risk arising on account of uncertainty, managements make use of enterprise risk management system. Internal audit is an integral part of this risk management system, an essential for ensuring its operating effectiveness and efficiency.

Internal audit is intricately woven into the fabric of management decision making in the entity and needs to understand and address the emerging concerns and issues of the entity at the earliest. Contemporary internal audit today is not, therefore, restricted only to the financial aspects of an entity, but penetrate deep into the operations as well. Internal audit is, accordingly, a highly specialized area, requiring high level of knowledge of the organisation and as well as its interrelationship with the variables in its operating environment. Since most of the modern entities employ advanced levels of technology in their operations, it is essential for the internal auditors to be well versed with its various facets and employ it in carrying out their internal audit.

Internal audit has been a core competence area of chartered accountants. Despite being given to work in multi disciplinary internal audit teams, chartered accountants have created a *niche* of their own in that area. To maintain that *niche*, it would be necessary for the chartered accountants to periodically assess their knowledge and skill up gradation requirements and undertaking such up gradation at the earliest. Thus, the process of

learning, unlearning and relearning for the internal auditors has to be a continuous one and critical to maintain that continuing utility to the entity.

It was primarily with this view that the Internal Audit Standards Board (constituted as the Committee on Internal Audit in 2004) of the Institute of Chartered Accountants of India decided to launch these training programmes on internal audit. It was understood that whereas bringing out technical literature was essential to expand the knowledge base of the members in the field of internal audit, it was equally necessary to have such training programmes, carried out by experienced faculty. Such training programmes are therefore not only aimed disseminating the technical developments among the members but also at providing practical implementation guidance to them. We firmly believe that a strong knowledge base backed by skill sets of contemporary relevance would provide better visibility and utility of the chartered accountants to the various stakeholders such as the entity's management as well as the regulators.

On the other hand, these programmes will also serve as fora to the Internal Audit Standards Board to understand/ identify the emerging areas of professional practice and concerns in the field of internal audit wherefor new/more technical literature and/ or such training needs to be imparted. This Training Material on Internal Audit is intended to serve as a source material to be used by the participants at the training programme. The material has been prepared by an expert and contains literature on a number of important issues which a contemporary internal auditor would need to be aware of.

At this juncture, I wish to express my sincere thanks to CA. Arijit Chakraborty, Kolkata who prepared this Training Material despite his demanding professional and personal preoccupations. I also wish to place on record my thanks to CA. Ved Jain, President and CA. Uttam P. Agarwal, Vice President, ICAI for their vision and support to the efforts of the Board. I am also thankful to my colleagues at the Internal Audit Standards Board for their guidance and support. I also wish to place my appreciation for the

efforts put in by CA. Puja Wadhera, Secretary, Internal Audit Standards Board and her team of officers, CA. Gurpreet Singh, Senior Executive Officer and CA. Arti Aggarwal, Executive Officer for giving final shape to this.

I am sure that this Training Material would be a fruitful resource material on internal audit for not only the participants but also other interested readers.

Kolkata
16th November, 2008

Abhijit Bandyopadhyay
Chairman,
Internal Audit Standards Board

GLOSSARY

Assurance	A positive confirmation intended to give confidence that what is reported may be relied upon.
Audit Plan	A list of audits to be carried out in a specified time frame.
Audit Universe	A list of all the audits required to provide assurance that all significant risks are properly managed.
Board	A board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a non-profit organization.
Control	Processes / activities which manage risks
Control Score (Gap)	The difference between the inherent and residual risk scores. The higher the value, the more important the control.
Director	Member of a controlling board, such as a company director, trustee, counselor or governor.
Enterprise-wide Risk Management (ERM)	A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats

	that affect the achievement of its objectives.
Inherent (Gross) Risk	The status of risk (measured through consequence and likelihood) without taking into account any risk management processes that the organization may already have in place.
Management of Risks	The implementation of responses to risks, which reduce their threat to below the level of the risk appetite or, where this is not possible, reports the risk to the board.
Monitoring	Processes which report to management, at appropriate intervals, the success, or otherwise, of the responses to risks.
Residual (Net) Risk	The status of risk (measured through consequence and likelihood) after taking into account any risk management processes that the organization may already have in place.
Risk	Circumstances / events which affect the achievement of objectives.
Risk Analysis	The systematic use of available information to determine the likelihood of specified events occurring and the magnitude of their consequences. Measured in terms of consequence and likelihood.
Risk Appetite	The level of risk that is acceptable to the board or

	management. This may be set in relation to the organization as a whole, for different groups of risks or at an individual risk level. Risks above the risk appetite are considered a threat to the reasonable assurance that an organization will achieve its objectives.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Risk and Audit Universe (RAU)	The risks register showing the audits which are intended to provide assurance that each risk is properly managed.
Risk Evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk Identification	The process of determining what can happen, why and how.
Risk-based Internal Auditing	The methodology which provides assurance that the risk management framework is operating as required by the board.
Risk Management Framework	The totality of the structures, methodology, procedures and definitions that an organization has chosen to use to implement its risk management processes.
Risk Management Processes	Processes to identify, assess, manage, and control

potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.

Risk Maturity

The extent to which a robust risk management approach has been adopted and applied, as planned, by management across the organization to identify, assess, decide on responses to and report on opportunities and threats that affect the achievement of the organization's objectives.

Risk Register

A complete list of risks, identified by management, which threaten the objectives and processes of the organization.

Risk Responses

The means by which an organization elects to manage individual risks. The main categories are to tolerate the risk; to treat it by reducing its impact or likelihood; to transfer it to another organization or to terminate the activity creating it. Internal controls are one way of treating a risk.

Significant Risk

A risk, inherent or residual, above the risk appetite.

CONTENTS

Foreword	(iii)
Preface.....	(v)
Glossary	(ix)

Module I: Evolution of Internal Audit – Past, Present and Future

Chapter I.1: Introduction to Internal Audit.....	3
Chapter I.2: Evolution of Corporate Governance and Internal Audit	8
Chapter I.3: Risk Management and Internal Audit.....	40
Chapter I.4: Sarbanes Oxley Act (SOX) – Milestone in the Perspective of Internal Audit.....	53
Chapter I.5: Discussions on Revised Clause 49.....	63
Chapter I.6: Audit Committee and Role of Internal Audit.....	68
Chapter I.7: Fraud Risk Management – Role of Internal Audit	71

Module II: Standards on Internal Audit

Preface to the Standards on Internal Audit.....	89
Framework for Standards on Internal Audit	97
SIA 1: Planning an Internal Audit.....	102
SIA 2: Basic Principles Governing Internal Audit	114
SIA 3: Documentation.....	120
SIA 4: Reporting	129
SIA 5: Sampling	138
SIA 6: Analytical Procedures	156
SIA 7: Quality Assurance in Internal Audit.....	165
SIA 8: Terms of Internal Audit Engagement	174

Module III: Managing the Internal Audit Activity

Chapter III.1: Introduction to Internal Audit Engagement Management.....	183
Chapter III.2: Internal Audit Planning	186
Chapter III.3: Internal Audit Program	194
Chapter III.4: Documentation.....	200
Chapter III.5: Sampling in Internal Audit	201
Chapter III.6: Risk Assessment and Internal Controls	204
Chapter III.7: Compliance Vs. Substantive Approach in Internal Audit.....	209
Chapter III.8: Issue Resolution and Obtaining Management Comments.....	215
Chapter III.9: Internal Audit Reporting	220

Module IV: Risk Analysis and Management, Risk-based Internal Audit

Chapter IV.1: Introduction to Risk-based Audit and Internal Audit.....	229
Chapter IV.2: Understanding Risk-based Internal Audit - Theory, Implications and Practical Issues	232
Chapter IV.3: Risk Management and Risk-based Internal Audit	239
Chapter IV.4: Risk-based Internal Auditing Application.....	247
Chapter IV.5: Planning and Scoping Multilocation RBIA Engagements – Important Considerations.....	257
Chapter IV.6: Risk Reporting	259
Chapter IV.7: Risk Evaluation Form (<i>Illustrative only</i>).....	265
Chapter IV.8: RBA / RBIA Templates, Flowcharts, Formats and Registers (<i>Illustrative list</i>)	277
Chapter IV.9: RBIA in Banks.....	287
Chapter IV.10: RBIA Questionnaire (<i>Illustrative only</i>)	294
Chapter IV.11: Risk Management Policy (<i>Illustrative</i>).....	296

Module V: Internal Control Framework – Understanding and Evaluation

Chapter V.1: Introduction to Internal Controls	309
Chapter V.2: Nature and Types of Internal Controls, Control Objectives and Activities	312
Chapter V.3: Understanding Control Frameworks – COSO Model	332
Chapter V.4: Control Self Assessments(CSA)	340
Chapter V.5: IT Controls and COBIT	343
Chapter V.6: Illustrations on Internal Control	353
Chapter V.7: Internal Controls and SOX	356
Chapter V.8: Control Evaluation Matrix	359
Chapter V.9: COSO Internal Control Checklists	381
Chapter V.10: SAS 70, Audit and Internal Control	385
Chapter V.11: Internal Controls and Fraud	389

Module VI: Internal Audit of Specific Functions: Finance and Accounts, Production, Marketing, Information Technology and Human Resource

Chapter VI.1: Internal Audit of Production and Operation	395
Chapter VI.2: Internal Audit of Marketing	414
Chapter VI.3: Internal Audit of Finance and Accounts	420
Chapter VI.4: Internal Audit of Human Resources	425
Chapter VI.5: Internal Audit of Information Technology	438
Chapter VI.6: Risk Templates, Risk Reporting	452

Module VII: Specialized Internal Audit – Due Diligence; Investigation; Fraud Detection; Concurrent Audit

Chapter VII.1: Introduction on Due Diligence	465
Chapter VII.2: Approach to Due Diligence	468
Chapter VII.3: Work Approach to Due Diligence	473

Chapter VII.4: Challenges and Risks Covered in Due Diligence Process.....	482
Chapter VII.5: Introduction of Fraud and Investigation.....	541
Chapter VII.6: Types of Frauds and Financial Crimes	544
Chapter VII.7: Red Flags in Detection of Frauds	549
Chapter VII.8: Steps in Conducting an Investigation.....	554
Chapter VII.9: Various Steps which can be Considered in a Situation of Fraud Detection	557
Chapter VII.10: Tools and Techniques Used	568
Chapter VII.11: Introduction of Concurrent Audit	586
Chapter VII.12: Objectives of Concurrent Audit	587
Chapter VII.13: Role of Concurrent Auditor	588

Module VIII: Internal Audit and Corporate Governance

Chapter VIII.1: Corporate Governance- An overview	639
Chapter VIII.2: Impact of Corporate Governance Requirements on Internal Audit.....	645
Chapter VIII.3: Role of Internal Audit in Strengthening Corporate Governance	650
Chapter VIII.4: Relationship Between the Audit Committee and Internal Auditor.....	652
Chapter VIII.5: Relationship Between the Board of Directors and Internal Auditor	654
Chapter VIII.6: Corporate Governance and Internal Control.....	655
Chapter VIII.7: Risk Management.....	658
Chapter VIII.8: Clause 49 – Corporate Governance	660

**EVOLUTION OF INTERNAL
AUDIT –PAST, PRESENT
AND FUTURE**

Chapter-I.1

Introduction to Internal Audit

The globalization of business, growing complexity of transactions and new-age IT infrastructure have revolutionized the concept of trade and commerce. However, parallel to this great upsurge, another growing factor has been haunting corporate board rooms—that is the phenomenon of ‘Risk’. This is an all pervading term covering operational, financial and regulatory domains. There can be a liquidity risk, a fraud risk, a reputational risk, a competition risk and sundry other forms of risk. To combat and reduce risk, managements have come up with better Internal Controls. As a corollary, the Internal Audit profession too has witnessed a sea-change from the traditional typical ‘compliance’ or ‘transaction’ audit to a much more dynamic ‘Risk-based Audit’, ‘Controls Assessments’, ‘Controls Rationalization’ and so forth.

The Changing Roles and Advent of Internal Audit

The Internal Audit Standards Board of the Institute of Chartered Accountants of India describes internal audit as *“Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system. Internal audit, therefore, provides assurance that there is transparency in reporting, as a part of good governance.”*

Internal auditing is a valuable resource to executive management and the board of directors (BoD) in accomplishing overall organizational goals and objectives, and simultaneously strengthening internal control and overall governance.

In the current global scenario, internal auditing function reviews the reliability and integrity of information, compliance with policies and regulations, the safeguarding of assets, the economical and

efficient use of resources, and established operational goals and objectives. Today, internal audits encompass all financial activities and operations including systems, production, engineering, marketing, and human resources. Indeed, a wide gamut of corporate activities.

The Value of Internal Audit in Audit Committees

The internal auditing function is of paramount importance to Audit Committees. The Audit Committee relies heavily on the internal auditor's assessment of risk and controls and draws heavily from their recommendations. Some quotes on internal audit's importance in Audit Committee:

"Internal audit is the primary resource of the audit committee in carrying out its duties and responsibilities. With those responsibilities increasing and continued pressure from the SEC for financial reporting integrity, a functioning partnership of the audit committee and internal audit is vital."

BellSouth Corporation

"An active and informed audit committee provides the ultimate independent and objective oversight of the corporate control environment, including focus on emerging trends and risks. Internal auditing is the primary agent of the audit committee within the company."

Ford Motor Company

Evolution of Internal Audit

K. H. Spencer Pickett¹, a noted author in the field of internal audit, has identified the following stages in the evolution of modern internal audit:

As a Sibling of External Audit

In the initial stages, internal audit began as an extended arm of an external/statutory audit of financial statements. The main, but

¹ The Essential Handbook of Internal Auditing, 2005 Edition.

rather restricted, function of the internal audit at this stage was verifying the reliability of the financial information included in the financial statements. The internal audit function in this stage of evolution could not understandably add much value to functioning of the entity.

As a Cross Check

In this stage of its evolution, internal audit was also required to test non-financial information and transactions in terms of their correctness and compliance with the laid down policies and procedures.

As a Probity Police

At this stage of its evolution, the internal audit came to be more concerned about the probity aspects of the transactions especially those involving liquid and highly movable assets such as cash, stocks, etc.

As a Non Financial Systems Police

As the global economy surged forward full steam, the need for having a full fledged, strategically directed internal audit emerged as an inevitable service that could assist managements in decision making, moving away from being merely a police on financial transactions. Thus, emerged the modern internal audit where the latter was established as a separate function, in house or outsourced, with clearly laid down missions and objectives to be achieved. As of today, internal audit undeniably is the backbone of a sound corporate governance system.

Factors Contributing to the Evolution of Internal Audit

Whereas in the preceding paragraphs the various stages in the evolution of internal audit have been discussed, the following are some of the factors, which have immensely contributed to that evolution.

Training Material on Internal Audit

Increased size and complexity of businesses

Increased size and business spread dilutes direct management oversight on various functions, necessitating the need for a full time, independent and dedicated team to review and appraise operations.

Enhanced compliance requirements

Increase in the geographical spread of the businesses has also led to crossing of political frontiers by businesses in a bid to tap global capital. This has thrown up compliance with the laws of the home country as well as the laws of that land as a critical factor for existence of businesses abroad.

Focus on risk management and internal controls to manage them

Internal auditors can carry out their job in a more focused manner by directing their efforts in the areas where there is a greater risk, thereby enhancing the overall efficiency of the process and adding greater value with the same set of resources.

Unconventional business models

Businesses today use unconventional models and practices, for example, outsourcing of non-core areas, such as accounting.

Intensive use of Information Technology

Information technology (IT) is invariably embedded in all spheres of activities of a modern business enterprise today, from data processing to resource planning to online sales and e-commerce. Use of IT has, however, increased the threat of data thefts or losses on account of systems failure or hacking/espionage, as well as the need to comply with the cyber laws, etc.

Stringent norms mandated by regulators to protect investors

The regulators are coming up in a big way to protect the interests of the investors. The focus of the latest regulations

being ethical conduct of business, and enhanced corporate governance and financial reporting requirements, etc.

An increasingly competitive environment

Whereas deregulation and globalization have melted the political as well as other barriers to entry in the markets for goods and services, free flow of capital, technology and know how among the countries as well as strong infrastructure has helped in bringing down the costs of production and better access to the existing and potential consumers. This in turn, has lured more and more players in the existing markets, thereby, stiffening the competition.

Need for internal audit to provide demonstrable value addition

1.18 Over the years, better corporate governance practices complemented by enhanced accounting and disclosure policies and practices codified in the form of Accounting Standards as well as immaculately designed advanced software packages for accounting and resource planning, have considerably brought down the need for the management to act as a police over the reliability and accuracy of the financial data. The internal audit has to, therefore focus, on areas other than financial data as well and help increase the stakeholders' value. One such focus area could be identifying areas of wastage of physical resources, deficiencies in internal controls, etc.

Conclusion - With this trend going on, it is observed that the internal audit has carved itself out as a distinct professional service and, in some respects, an unique profession altogether. The ICAI, in its pioneering role has already issued eight Standards on Internal Audit.

Chapter-I.2

Evolution of Corporate Governance and Internal Audit

Corporate Governance has been attracting public attention across the world. High profile financial reporting failures in developed markets, scandals and financial crisis in emerging markets have put corporate and governmental oversight in spotlight. The quality of governance is indispensable to shape the growth and the future of any capital market, economy and organization.

Corporate Governance may be defined as *“A set of systems, processes and principles source which ensure that a company is governed in the best interest of all stakeholders.”* It ensures commitment to values and ethical conduct of business; transparency in business transactions; statutory and legal compliance; adequate disclosures and effective decision-making to achieve corporate objectives. In other words, Corporate Governance is about promoting corporate fairness, transparency and accountability.

The framework of corporate governance is built around the following elements:

- Supervisory Board/ Committee/ Team
- Audit Committee
- Internal Audit
- Statutory / External Audit
- Disclosure of information
- Risk management framework
- Internal control framework
- Anti-fraud programs

- Whistle blower policy
- Control Self-assessments

The stakeholders to corporate governance include:

- Board of Directors
- Executive Managers
- Workers / Employees
- Shareholders or Owners
- Regulators
- Customers
- Suppliers
- Community (people affected by the actions of the organization)

Evolution of Corporate Governance

Kautilya's (Chanakya) *Arthashastra* is the oldest book (around 300 B.C) on Management available to the world, covering a wide range of critical recommendations such as:

- the king shall not consult with any advisor who had a vested interest in the outcome of a particular project.
- establishment of an ***ethical code of conduct***—a topic which has received a great deal of attention now during the past few years after corporate scandals.
- the ***codification of accounting rules*** into one uniform system to prevent problems in translating financial data between disparate methods of accounting – a subject which the international accounting community is dealing with in terms of the convergence of accounting standards.

In the **western world**, the East India Company introduced a Court of Directors, separating ownership and control in 1600s.

International Milestones in Corporate Governance

Year	Name of Committee/ Body	Areas / Aspects Covered
1992	Sir Adrian Cadbury Committee, UK	Financial Aspects of Corporate Governance
1994	Mervyn E. King's Committee, South Africa	Corporate Governance
1995	Greenbury Committee, UK	Directors' Remuneration
1998	Hampel Committee, UK	Combine Code of Best Practices
1999	Blue Ribbon Committee, US	Improving the Effectiveness of Corporate Audit Committees
1999	OECD	Principles of Corporate Governance
1999	CACG	Principles for Corporate Governance in Commonwealth
2003	Derek Higgs Committee, UK	Review of role of effectiveness of Non-executive Directors
2003	ASX Corporate Governance Council, Australia	Principles of Good Corporate Governance and Best Practice Recommendations

The Indian Scenario – Down the Years

Year	Name of Committee/Body	Areas/Aspects Covered
1998	Confederation of Indian Industry (CII)	Desirable Corporate Governance – A Code
1999	Kumar Mangalam Birla Committee	Corporate Governance
2002	Naresh Chandra Committee	Corporate Audit and Governance
2003	N. R. Narayana Murthy Committee	Corporate Governance

Clause 49 - Corporate Governance

The company agrees to comply with the following provisions:

I. Board of Directors

(A) Composition of Board

- (i) The board of directors of the company shall have an optimum combination of executive and non-executive directors with not less than fifty percent of the board of directors comprising of non-executive directors.
- (ii) Where the Chairman of the Board is a non-executive director, at least one-third of the board should comprise of independent directors and in case he is an executive director, at least half of the board should comprise of independent directors.
- (iii) For the purpose of the sub-clause (ii), the expression 'independent director' shall mean a non-executive director of the company who:
 - a. apart from receiving director's remuneration, does not have any material pecuniary relationships or

Training Material on Internal Audit

transactions with the company, its promoters, its directors, its senior management or its holding company, its subsidiaries and associates which may affect independence of the director;

- b. is not related to promoters or persons occupying management positions at the board level or at one level below the board;
- c. has not been an executive of the company in the immediately preceding three financial years;
- d. is not a partner or an executive or was not partner or an executive during the preceding three years, of any of the following:
 - i) the statutory audit firm or the internal audit firm that is associated with the company, and
 - ii) the legal firm(s) and consulting firm(s) that have a material association with the company.
- e. is not a material supplier, service provider or customer or a lessor or lessee of the company, which may affect independence of the director; and
- f. is not a substantial shareholder of the company i.e. owning two percent or more of the block of voting shares.

Explanation

For the purposes of the sub-clause (iii):

- a. Associate shall mean a company which is an “associate” as defined in Accounting Standard (AS) 23, “Accounting for Investments in Associates in Consolidated Financial Statements”, issued by the Institute of Chartered Accountants of India.
- b. “Senior management” shall mean personnel of the company who are members of its core management team excluding board of directors. Normally, this would

comprise all members of management one level below the executive directors, including all functional heads.

c. "Relative" shall mean "relative" as defined in section 2(41) and section 6 read with Schedule IA of the Companies Act, 1956.

(iv) Nominee directors appointed by an institution which has invested in or lent to the company shall be deemed to be independent directors.

Explanation

"Institution" for this purpose means a public financial institution as defined in Section 4A of the Companies Act, 1956 or a "corresponding new bank" as defined in section 2(d) of the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970 or the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980 [both Acts]."

(B) Non executive directors' compensation and disclosures

All fees/compensation, if any paid to non-executive directors, including independent directors, shall be fixed by the board of directors and shall require previous approval of shareholders in general meeting. The shareholders' resolution shall specify the limits for the maximum number of stock options that can be granted to non-executive directors, including independent directors, in any financial year and in aggregate.

(C) Other provisions as to Board and Committees

- (i) The board shall meet at least four times a year, with a maximum time gap of three months between any two meetings. The minimum information to be made available to the board is given in **Annexure– I A**.
- (ii) A director shall not be a member in more than 10 committees or act as Chairman of more than five committees across all companies in which he is a director.

Furthermore it should be a mandatory annual requirement for every director to inform the company about the committee positions he occupies in other companies and notify changes as and when they take place.

Explanation

1. For the purpose of considering the limit of the committees on which a director can serve, all public limited companies, whether listed or not, shall be included and all other companies including private limited companies, foreign companies and companies under Section 25 of the Companies Act shall be excluded.
 2. For the purpose of reckoning the limit under this sub-clause, Chairmanship/ membership of the Audit Committee and the Shareholders' Grievance Committee alone shall be considered.
- (iii) The Board shall periodically review compliance reports of all laws applicable to the company, prepared by the company as well as steps taken by the company to rectify instances of non-compliances.

(D) Code of Conduct

- (i) The Board shall lay down a code of conduct for all Board members and senior management of the company. The code of conduct shall be posted on the website of the company.
- (ii) All Board members and senior management personnel shall affirm compliance with the code on an annual basis. The Annual Report of the company shall contain a declaration to this effect signed by the CEO.

Explanation

For this purpose, the term "senior management" shall mean personnel of the company who are members of its core management team excluding Board of Directors. Normally, this would comprise all members of management one level below the executive directors, including all functional heads.

II. Audit Committee

(A) Qualified and Independent Audit Committee

A qualified and independent audit committee shall be set up, giving the terms of reference subject to the following:

- (i) The audit committee shall have minimum three directors as members. Two-thirds of the members of audit committee shall be independent directors.
- (ii) All members of audit committee shall be financially literate and at least one member shall have accounting or related financial management expertise.

Explanation 1

The term “financially literate” means the ability to read and understand basic financial statements i.e. balance sheet, profit and loss account, and statement of cash flows.

Explanation 2

A member will be considered to have accounting or related financial management expertise if he or she possesses experience in finance or accounting, or requisite professional certification in accounting, or any other comparable experience or background which results in the individual's financial sophistication, including being or having been a chief executive officer, chief financial officer or other senior officer with financial oversight responsibilities.

- (iii) The chairman of the audit committee shall be an independent director;
- (iv) The chairman of the audit committee shall be present at annual general meeting to answer shareholder queries;
- (v) The audit committee may invite such of the executives, as it considers appropriate (and particularly the head of the finance function) to be present at the meetings of the committee, but on occasions it may also meet without the

Training Material on Internal Audit

presence of any executives of the company. The finance director, head of internal audit and a representative of the statutory auditor may be present as invitees for the meetings of the audit committee;

- (vi) The Company Secretary shall act as the secretary to the committee.

(B) Meeting of Audit Committee

The audit committee should meet at least four times in a year and not more than four months shall elapse between two meetings. The quorum shall be either two members or one third of the members of the audit committee whichever is greater, but there should be a minimum of two independent members present.

(C) Powers of Audit Committee

The audit committee shall have powers, which should include the following:

1. To investigate any activity within its terms of reference.
2. To seek information from any employee.
3. To obtain outside legal or other professional advice.
4. To secure attendance of outsiders with relevant expertise, if it considers necessary.

(D) Role of Audit Committee

The role of the audit committee shall include the following:

1. Oversight of the company's financial reporting process and the disclosure of its financial information to ensure that the financial statement is correct, sufficient and credible.
2. Recommending to the Board, the appointment, re-appointment and, if required, the replacement or removal of the statutory auditor and the fixation of audit fees.

Evolution of Corporate Governance and Internal Audit

3. Approval of payment to statutory auditors for any other services rendered by the statutory auditors.
4. Reviewing, with the management, the annual financial statements before submission to the board for approval, with particular reference to:
 - a. Matters required to be included in the Director's Responsibility Statement to be included in the Board's report in terms of clause (2AA) of section 217 of the Companies Act, 1956.
 - b. Changes, if any, in accounting policies and practices and reasons for the same.
 - c. Major accounting entries involving estimates based on the exercise of judgment by management.
 - d. Significant adjustments made in the financial statements arising out of audit findings.
 - e. Compliance with listing and other legal requirements relating to financial statements.
 - f. Disclosure of any related party transactions g. Qualifications in the draft audit report.
5. Reviewing, with the management, the quarterly financial statements before submission to the board for approval.
6. Reviewing, with the management, performance of statutory and internal auditors, adequacy of the internal control systems.
7. Reviewing the adequacy of internal audit function, if any, including the structure of the internal audit department, staffing and seniority of the official heading the department, reporting structure coverage and frequency of internal audit.
8. Discussion with internal auditors any significant findings and follow up there on.
9. Reviewing the findings of any internal investigations by the

Training Material on Internal Audit

internal auditors into matters where there is suspected fraud or irregularity or a failure of internal control systems of a material nature and reporting the matter to the board.

10. Discussion with statutory auditors before the audit commences , about the nature and scope of audit as well as post-audit discussion to ascertain any area of concern.
11. To look into the reasons for substantial defaults in the payment to the depositors, debenture holders, shareholders (in case of non payment of declared dividends) and creditors.
12. To review the functioning of the Whistle Blower mechanism, in case the same is existing.
13. Carrying out any other function as is mentioned in the terms of reference of the Audit Committee.

Explanation (i)

The term "related party transactions" shall have the same meaning as contained in the Accounting Standard 18, Related Party Transactions, issued by The Institute of Chartered Accountants of India.

Explanation (ii)

If the company has set up an audit committee pursuant to provision of the Companies Act, the said audit committee shall have such additional functions features as is contained in this clause.

(E) Review of information by Audit Committee

The Audit Committee shall mandatorily review the following information:

1. Management discussion and analysis of financial condition and results of operations;
2. Statement of significant related party transactions (as defined by the audit committee), submitted by management;
3. Management letters / letters of internal control weaknesses

issued by the statutory auditors;

4. Internal audit reports relating to internal control weaknesses; and
5. The appointment, removal and terms of remuneration of the Chief internal auditor shall be subject to review by the Audit Committee

III. Subsidiary Companies

- i. At least one independent director on the Board of Directors of the holding company shall be a director on the Board of Directors of a material non listed Indian subsidiary company.
- ii. The Audit Committee of the listed holding company shall also review the financial statements, in particular, the investments made by the unlisted subsidiary company.
- iii. The minutes of the Board meetings of the unlisted subsidiary company shall be placed at the Board meeting of the listed holding company. The management should periodically bring to the attention of the Board of Directors of the listed holding company, a statement of all significant transactions and arrangements entered into by the unlisted subsidiary company.

Explanation 1

The term “material non-listed Indian subsidiary” shall mean an unlisted subsidiary, incorporated in India, whose turnover or net worth (i.e. paid up capital and free reserves) exceeds 20% of the consolidated turnover or net worth respectively, of the listed holding company and its subsidiaries in the immediately preceding accounting year.

Explanation 2

The term “significant transaction or arrangement” shall mean any individual transaction or arrangement that exceeds or is likely to exceed 10% of the total revenues or total expenses or total assets or total liabilities, as the case may be, of the material

unlisted subsidiary for the immediately preceding accounting year.

Explanation 3

Where a listed holding company has a listed subsidiary which is itself a holding company, the above provisions shall apply to the listed subsidiary insofar as its subsidiaries are concerned.

IV. Disclosures

(A) Basis of related party transactions

- (i) A statement in summary form of transactions with related parties in the ordinary course of business shall be placed periodical ly before the audit committee.
- (ii) Details of m aterial individual transactions with related parties which are not in the normal course of business shall be placed before the audit committee.
- (iii) Details of material individual transactions with related parties or others, which are not on an arm's length basis should be placed before the audit committee, together with Management's justification for the same.

(B) Disclosure of Accounting Treatment

Where in the preparation of financial statements, a treatment different from that prescribed in an Accounting Standard has been followed, the fact shall be disclosed in the financial statements, together with the management's explanation as to why it believes such alternative treatment is more representative of the true and fair view of the underlying business transaction in the Corporate Governance Report.

(C) Board Disclosures – Risk management

The company shall lay down procedures to inform Board members about the risk assessment and minimization

procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework.

(D) Proceeds from public issues, rights issues, preferential issues etc.

When money is raised through an issue (public issues, rights issues, preferential issues etc.), it shall disclose to the Audit Committee, the uses / applications of funds by major category (capital expenditure, sales and marketing, working capital, etc), on a quarterly basis as a part of their quarterly declaration of financial results. Further, on an annual basis, the company shall prepare a statement of funds utilized for purposes other than those stated in the offer document/prospectus /notice and place it before the audit committee. Such disclosure shall be made only till such time that the full money raised through the issue has been fully spent. This statement shall be certified by the statutory auditors of the company. The audit committee shall make appropriate recommendations to the Board to take up steps in this matter.

(E) Remuneration of Directors

- (i) All pecuniary relationship or transactions of the non-executive directors *vis-à-vis* the company shall be disclosed in the Annual Report.
- (ii) Further the following disclosures on the remuneration of directors shall be made in the section on the corporate governance of the Annual Report:
 - (a) All elements of remuneration package of individual directors summarized under major groups, such as salary, benefits, bonuses, stock options, pension etc.
 - (b) Details of fixed component and performance linked incentives, along with the performance criteria.
 - (c) Service contracts, notice period, severance fees.
 - (d) Stock option details, if any – and whether issued at a discount as well as the period over which accrued

and over which exercisable.

- (iii) The company shall publish its criteria of making payments to non-executive directors in its annual report. Alternatively, this may be put up on the company's website and reference drawn thereto in the annual report.
- (iv) The company shall disclose the number of shares and convertible instruments held by non-executive directors in the annual report.
- (v) Non-executive directors shall be required to disclose their shareholding (both own or held by / for other persons on a beneficial basis) in the listed company in which they are proposed to be appointed as directors, prior to their appointment. These details should be disclosed in the notice to the general meeting called for appointment of such director.

(F) Management

- (i) As part of the directors' report or as an addition thereto, a Management Discussion and Analysis report should form part of the Annual Report to the shareholders. This Management Discussion and Analysis should include discussion on the following matters within the limits set by the company's competitive position:
 - a. Industry structure and developments.
 - b. Opportunities and Threats.
 - c. Segment-wise or product-wise performance.
 - d. Outlook.
 - e. Risks and concerns.
 - f. Internal control systems and their adequacy.
 - g. Discussion on financial performance with respect to operational performance.
 - h. Material developments in Human Resources / Industrial

Relations front, including number of people employed.

- (ii) Senior management shall make disclosures to the board relating to all material financial and commercial transactions, where they have personal interest, that may have a potential conflict with the interest of the company at large (for e.g. dealing in company shares, commercial dealings with bodies, which have shareholding of management and their relatives etc.).

Explanation

For this purpose, the term "senior management" shall mean personnel of the company who are members of its core management team excluding the Board of Directors). This would also include all members of management one level below the executive directors including all functional heads.

(G) Shareholders

- (i) In case of the appointment of a new director or re-appointment of a director the shareholders must be provided with the following information:
 - (a) A brief resume of the director;
 - (b) Nature of his expertise in specific functional areas;
 - (c) Names of companies in which the person also holds the directorship and the membership of Committees of the Board; and
 - (d) Shareholding of non-executive directors as stated in Clause 49 (IV) (E) (v) above
- (ii) Quarterly results and presentations made by the company to analysts shall be put on company's web-site, or shall be sent in such a form so as to enable the stock exchange on which the company is listed to put it on its own web-site.
- (iii) A board committee under the chairmanship of a non-executive director shall be formed to specifically look into the redressal of shareholder and investors complaints like

transfer of shares, non-receipt of balance sheet, non-receipt of declared dividends etc. This Committee shall be designated as 'Shareholders / Investors Grievance Committee'.

- (iv) To expedite the process of share transfers, the Board of the company shall delegate the power of share transfer to an officer or a committee or to the registrar and share transfer agents. The delegated authority shall attend to share transfer formalities at least once in a fortnight.

V. CEO/CFO certification

The CEO, i.e. the Managing Director or Manager appointed in terms of the Companies Act, 1956 and the CFO i.e. the whole-time Finance Director or any other person heading the finance function discharging that function shall certify to the Board that:

- (a) They have reviewed financial statements and the cash flow statement for the year and that to the best of their knowledge and belief :
 - (i) these statements do not contain any materially untrue statement or omit any material fact or contain statements that might be misleading; and
 - (ii) these statements together present a true and fair view of the company's affairs and are in compliance with existing accounting standards, applicable laws and regulations.
- (b) There are, to the best of their knowledge and belief, no transactions entered into by the company during the year which are fraudulent, illegal or violative of the company's code of conduct.
- (c) They accept responsibility for establishing and maintaining internal controls and that they have evaluated the effectiveness of the internal control systems of the company and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of

internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies.

- (d) They have indicated to the auditors and the Audit committee:
 - (i) significant changes in internal control during the year;
 - (ii) significant changes in accounting policies during the year and that the same have been disclosed in the notes to the financial statements; and
 - (iii) Instances of significant fraud of which they have become aware and the involvement therein, if any, of the management or an employee having a significant role in the company's internal control system

VI. Report on Corporate Governance

- (i) There shall be a separate section on Corporate Governance in the Annual Reports of company, with a detailed compliance report on Corporate Governance. Non-compliance of any mandatory requirement of this clause with reasons thereof and the extent to which the non-mandatory requirements have been adopted should be specifically highlighted. The suggested list of items to be included in this report is given in **Annexure- I C** and list of non-mandatory requirements is given in **Annexure – I D**.
- (ii) The companies shall submit a quarterly compliance report to the stock exchanges within 15 days from the close of quarter as per the format given in **Annexure I B**. The report shall be signed either by the Compliance Officer or the Chief Executive Officer of the company.

VII. Compliance

- (1) The company shall obtain a certificate from either the

Training Material on Internal Audit

auditors or practicing company secretaries regarding compliance of conditions of corporate governance as stipulated in this clause and annex the certificate with the directors' report, which is sent annually to all the shareholders of the company. The same certificate shall also be sent to the Stock Exchanges along with the annual report filed by the company.

- (2) The non-mandatory requirements given in **Annexure – I D** may be implemented as per the discretion of the company. However, the disclosures of the compliance with mandatory requirements and adoption (and compliance) / non-adoption of the non-mandatory requirements shall be made in the section on corporate governance of the Annual Report.

ANNEXURE I A

Information to be placed before Board of Directors

1. Annual operating plans and budgets and any updates.
2. Capital budgets and any updates.
3. Quarterly results for the company and its operating divisions or business segments.
4. Minutes of meetings of audit committee and other committees of the board.
5. The information on recruitment and remuneration of senior officers just below the board level, including appointment or removal of Chief Financial Officer and the Company Secretary.
6. Show cause, demand, prosecution notices and penalty notices which are material ly important.
7. Fatal or serious accidents, dangerous occurrences, any material effluent or pollution problems.
8. Any material default in financial obligations to and by the company, or substantial non- payment for goods sold by the company.
9. Any issue, which involves possible public or product liability claims of substantial nature, including any judgement or order which, may have passed strictures on the conduct of the company or taken an adverse view regarding another enterprise that can have negative implications on the company.
10. Details of any joint venture or collaboration agreement.
11. Transactions that involve substantial payment towards goodwill, brand equity, or intellectual property.

Training Material on Internal Audit

12. Significant labour problems and their proposed solutions. Any significant development in Human Resources/ Industrial Relations front like signing of wage agreement, implementation of Voluntary Retirement Scheme etc.
13. Sale of material nature, of investments, subsidiaries, assets, which is not in normal course of business.
14. Quarterly details of foreign exchange exposures and the steps taken by management to limit the risks of adverse exchange rate movement, if material.
15. Non-compliance of any regulatory, statutory or listing requirements and shareholders service such as non-payment of dividend, delay in share transfer etc.

ANNEXURE I B

**Format of Quarterly Compliance Report
on Corporate Governance**

Name of the Company:

Quarter ending on:

Particulars	Clause of Listing agreement	Compliance Status Yes/No	Remarks
I. Board of Directors	49I		
(A) Composition of Board	49(IA)		
(B) Non-executive Directors'	49 (IB)		
(C) Other provisions as to Board and Committees	49 (IC)		
(D) Code of Conduct	49 (ID)		
II. Audit Committee	49 (II)		
(A) Qualified and Independent Audit Committee	49 (IIA)		
(B) Meeting of Audit Committee	49 (IIB)		
(C) Powers of Audit Committee	49 (IIC)		
(D) Role of Audit Committee	49 II(D)		
(E) Review of Information by Audit Committee	49 (IIE)		

Training Material on Internal Audit

III. Subsidiary Companies	49 (III)		
IV. Disclosures	49 (IV)		
(A) Basis of related party transactions	49 (IV A)		
(B) Board Disclosures	49 (IV B)		
(C) Proceeds from public issues, rights issues , preferential issues etc.	49 (IV C)		
(D) Remuneration of Directors	49 (IV D)		
(E) Management	49 (IV E)		
(F) Shareholders	49 (IV F)		
V. CEO/CFO Certification	49 (V)		
VI. Report on Corporate Governance	49 (VI)		
VII. Compliance	49 (VII)		

Note:

- 1) *The details under each head shall be provided to incorporate all the information required as per the provisions of the Clause 49 of the Listing Agreement.*
- 2) *In the column No.3, compliance or non-compliance may be indicated by Yes/No/N.A. For example, if the Board has been composed in accordance with the Clause 49 I of the Listing Agreement, "Yes" may be indicated. Similarly, in case the company has no related party transactions, the words "N.A." may be indicated against 49 (IV A).*
- 3) In the remarks column, reasons for non-compliance may be indicated, for example, in case of requirement related to circulation of information to the shareholders, which would be done only in the AGM/EGM, it might be indicated in the

Evolution of Corporate Governance and Internal Audit

"Remarks" column as – "will be complied with at the AGM". Similarly, in respect of matters which can be complied with only where the situation arises, for example, "Report on Corporate Governance" is to be a part of Annual Report only, the words "will be complied in the next Annual Report" may be indicated.

ANNEXURE I C

Suggested List of Items to Be Included In the Report on Corporate Governance in the Annual Report of Companies

- 1. A brief statement on company's philosophy on code of governance.**
- 2. Board of Directors:**
 - i. Composition and category of directors, for example, promoter, executive, non-executive, independent non-executive, nominee director, which institution represented as lender or as equity investor.
 - ii. Attendance of each director at the Board meetings and the last AGM.
 - iii. Number of other Boards or Board Committees in which he/she is a member or Chairperson.
 - iv. Number of Board meetings held, dates on which held.
- 3. Audit Committee:**
 - i. Brief description of terms of reference.
 - ii. Composition, name of members and Chairperson.
 - iii. Meetings and attendance during the year.
- 4. Remuneration Committee:**
 - i. Brief description of terms of reference.
 - ii. Composition, name of members and Chairperson.
 - iii. Attendance during the year.
 - iv. Remuneration policy.
 - v. Details of remuneration to all the directors, as per format in main report.

5. Shareholders Committee:

- i. Name of non-executive director heading the committee.
- ii. Name and designation of compliance officer.
- iii. Number of shareholders' complaints received so far.
- iv. Number not solved to the satisfaction of shareholders
Number of pending complaints.

6. General Body meetings:

- i. Location and time, where last three AGMs held.
- ii. Whether any special resolutions passed in the previous 3 AGMs.
- iii. Whether any special resolution passed last year through postal ballot – details of voting pattern.
- iv. Person who conducted the postal ballot exercise.
- v. Whether any special resolution is proposed to be conducted through postal ballot.
- vi. Procedure for postal ballot.

7. Disclosures:

- i. Disclosures on materially significant related party transactions that may have potential conflict with the interests of company at large.
- ii. Details of non-compliance by the company, penalties, strictures imposed on the company by Stock Exchange or SEBI or any statutory authority, on any matter related to capital markets, during the last three years. Whistle Blower policy and affirmation that no personnel has been denied access to the audit committee.
- iii. Details of compliance with mandatory requirements and adoption of the non-mandatory requirements of this clause.

8. Means of communication.

- i. Quarterly results;
- ii. Newspapers wherein results normally published;
- iii. Any website, where displayed;
- iv. Whether it also displays official news releases; and
- v. The presentations made to institutional investors or to the analysts.

9. General Shareholder information:

- i. AGM : Date, time and venue.
- ii. Financial year.
- iii. Date of Book closure.
- iv. Dividend Payment Date.
- v. Listing on Stock Exchanges.
- vi. Stock Code.
- vii. Market Price Data : High., Low during each month in last financial year.
- viii. Performance in comparison to broad -based indices such as BSE Sensex, CRISIL index etc.
- ix. Registrar and Transfer Agents.
- x. Share Transfer System.
- xi. Distribution of shareholding.
- xii. Dematerialization of shares and liquidity.
- xiii. Outstanding GDRs/ADRs/Warrants or any Convertible instruments, conversion date and likely impact on equity.
- xiv. Plant Locations.
- xv. Address for correspondence.

ANNEXURE I D

Non-Mandatory Requirements

(1) The Board

A non-executive Chairman may be entitled to maintain a Chairman's office at the company's expense and also allowed reimbursement of expenses incurred in performance of his duties.

Independent Directors may have a tenure not exceeding, in the aggregate, a period of nine years, on the Board of a company.

(2) Remuneration Committee

- i. The board may set up a remuneration committee to determine on their behalf and on behalf of the shareholders with agreed terms of reference, the company's policy on specific remuneration packages for executive directors including pension rights and any compensation payment.
- ii. To avoid conflicts of interest, the remuneration committee, which would determine the remuneration packages of the executive directors may comprise of at least three directors, all of whom should be non-executive directors, the Chairman of committee being an independent director.
- iii. All the members of the remuneration committee could be present at the meeting.
- iv. The Chairman of the remuneration committee could be present at the Annual General Meeting, to answer the shareholder queries. However, it would be up to the Chairman to decide who should answer the queries.

(3) Shareholder Rights

A half-yearly declaration of financial performance including summary of the significant events in last six-months, may be sent to each household of shareholders.

(4) Audit Qualifications

Company may move towards a regime of unqualified financial statements.

(5) Training of Board Members

A company may train its Board members in the business model of the company as well as the risk profile of the business parameters of the company, their responsibilities as directors, and the best ways to discharge them.

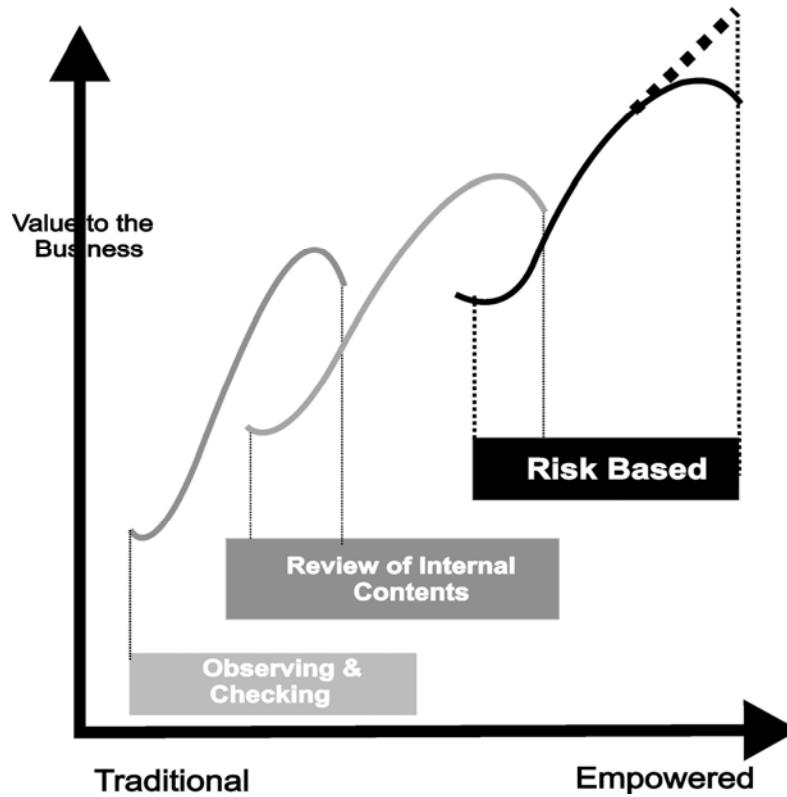
(6) Mechanism for Evaluating Non-executive Board Members

The performance evaluation of non-executive directors could be done by a peer group comprising the entire Board of Directors, excluding the director being evaluated; and Peer Group evaluation could be the mechanism to determine whether to extend / continue the terms of appointment of non-executive directors.

(7) Whistle Blower Policy

The company may establish a mechanism for employees to report to the management concerns about unethical behaviour, actual or suspected fraud or violation of the company's code of conduct or ethics policy. This mechanism could also provide for adequate safeguards against victimization of employees who avail of the mechanism and also provide for direct access to the Chairman of the Audit committee in exceptional cases. Once established, the existence of the mechanism may be appropriately communicated within the organization.

Evolution of Internal Audit



Feature	Old paradigm	New paradigm
Focus	Internal control	Business risk
Response	Reactive, after the fact	Proactive, continuous
Role	Independent appraisal function	Risk management
Recommendations / deliverables	Internal Control: <ul style="list-style-type: none"> ➤ Strengthen ➤ Cost – Benefit ➤ Efficiency and effectiveness 	Risk management: <ul style="list-style-type: none"> ➤ Avoid / diversify risk ➤ Share / transfer risk ➤ Control / accept risk

Internal Audit – Emerging Roles

Communication

This involves:

- Keeping senior management aware of critical issues.
- Ensuring factual communications of financial and other data.
- Providing suggestions based on knowledge of operations throughout the organization.

Compliance

The 'Compliance' aspect of internal audit involves:

- Ensuring management's policies and procedures are followed.
- Analysing impact of changes in procedures.
- Evaluating compliance with laws and regulations.
- Reviewing objectives for adherence to organization's mission and culture.
- Providing insight to the impact of noncompliance.

In contemporary times, internal auditor's reporting responsibilities.

- To the Audit Committee is increasing though administrative reporting to Finance function has not changed significantly
- The Chief Internal Auditor, therefore, must have a strong and direct reporting relationship with the audit committee; and the audit committee must take responsibility for certain supervisory activities, including approving internal audit's budget, risk assessment, audit plan, and for hiring, evaluating, and, if necessary, firing the CAE.

- Having a dual reporting relationship to the CEO can facilitate the required administrative activities associated with operating the function within the company.

Internal Audit Changing Trends - Extracts from a Big 4 Survey (?)

Expectations from Internal Audit Function

Respondents agree that in today's changing business arena there is a greater need and a greater opportunity for the *Internal Audit* function to contribute more. One important way to meet these expectations is to refocus Internal Audit on the critical risks and exposures that can determine an organization's success or failure.

Survey statistics –

	Total (%)	Senior Executives (%)	Internal Audit Management (%)
Good understanding of business issues	69	66	72
Proactive communication	66	62	70
Able to assess and help manage business risks	58	50	66
Proactive in meeting senior management requirements	52	44	59
Working effectively with all units/divisions	52	48	56
Innovation	37	30	44
Identifying profit improvement opportunities	30	31	28

Chapter-I.3

Risk Management and Internal Audit

Risk Management is the process of measuring or assessing risk and developing strategies to manage it. Strategies include –

- i) transferring the risk to another party,
- ii) avoiding the risk,
- iii) reducing the negative effect of the risk, and
- iv) accepting some or all of the consequences of a particular risk.

Traditional Risk Management focuses on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death, and lawsuits).

Financial Risk Management focuses on risks that can be managed using traded financial instruments. In an ideal risk management case, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled later.

Intangible Risk Management identifies a new type of risk - a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, knowledge risk occurs when deficient knowledge is applied.

Relationship Risk occurs when collaboration ineffectiveness occurs.

Process-engagement Risk occurs when operational ineffectiveness occurs. These risks directly reduce the productivity of knowledge workers, decrease cost effectiveness, profitability, service, quality, reputation, brand value, and earnings quality.

Steps in the Enterprise Risk Management Process

Step -1 : Establish the context

Establishing the context includes planning the remainder of the process and mapping out the scope of the exercise, the identity and objectives of stakeholders, the basis upon which risks will be evaluated and defining a framework for the process, and agenda for identification and analysis of risk involved in the process.

Step -2 : Identification

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems. Hence, risk identification can start with the source of problems, or with the problem itself.

- **Source analysis** Risk sources may be internal or external to the system that is the target of risk management. Examples of risk sources are: stakeholders of a project, employees of a company or the weather over an airport.
- **Problem analysis** Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of privacy information or the threat of accidents and casualties. The threats may exist with various entities, most important with shareholder, customers and legislative bodies such as the government.

When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example: stakeholders withdrawing during a project may endanger funding of the project; privacy information may be stolen by employees even within a closed network, etc.

The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for

identifying source, problem or event. Common risk identification methods are:

- **Objectives-based Risk Identification** Organizations and project teams have objectives. Any event that may endanger achieving an objective partly or completely is identified as risk. Objective-based risk identification is at the basis of COSO's ERM –An Integrated Framework.
- **Scenario-based Risk Identification** In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk

Step- 3 : Risk assessment

Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation of the Risk Management Plan.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for immaterial assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized.

Rate Of Occurrence Multiplied By The Impact Of The Event Equals Risk

Step-4 : Potential risk treatments

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories: (Dorfman, 1997)

- Tolerate
- Treat(i.e., Mitigation)
- Terminate(i.e., Retention)
- Transfer

Ideal use of these strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions.

Risk avoidance - Includes not performing an activity that could carry risk.

Risk reduction - Involves methods that reduce the severity of the loss.

Risk retention- Involves accepting the loss when it occurs..

Risk transfer- Means causing another party to accept the risk, typically by contract or by hedging.

Step-5 : Creating The Plan

The combination of methods to be used for each risk needs to be decided. Each risk management decision should be recorded and approved by the appropriate level of management. For example, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks. The plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of

computer viruses could be mitigated by acquiring and implementing anti virus software.

Step-6 : Implementation and Reporting

By following all of the planned methods for mitigating the effect of the risks, purchasing insurance policies for the risks that have been decided to be transferred to an insurer, risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest.

Step-7: Review and Evaluation of the Plan

Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

A diagrammatic representation is as follows –

The Risk Management Process



Areas of Risk Management

In corporate finance, risk management is a technique for measuring, monitoring and controlling the financial or operational risk on a firm's balance sheet. The Basel II framework breaks risks into –

- Market risk (price risk),
- Credit risk and
- Operational risk and also specifies methods for calculating capital requirements for each of these components.

Enterprise Risk Management (ERM)

In ERM, risk is defined as a possible event or circumstance that can have negative influences on the enterprise in question. Its impact can be on the very existence, the resources (human and capital), the products and services, or the customers of the enterprise, as well as external impacts on society, markets or the environment.

Risk Management Activities as Applied to Project Management

These activities would include:

- Plan should include risk management tasks, responsibilities, activities and budget.
- Assigning a risk officer - a team member other than a project manager who is responsible for foreseeing potential project problems.
- Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance.
- Creating anonymous risk reporting channel. Each team member should have possibility to report risk that he foresees in the project.

- Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by who and how will be done to avoid it or minimize consequences if it becomes a liability.
- Summarizing planned and faced risks, effectiveness of mitigation activities and effort spend for the risk management.

Risk Management and Business Continuity Planning (BCP)

Risk management is simply a practice of systematically selecting cost effective approaches for minimizing the effect of threat realization to the organization. All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore all organizations have to accept some level of *residual* risks.

Whereas risk management tends to be pre-emptive, BCP was invented to deal with the consequences of realised residual risks. The necessity to have BCP in place arises because even very unlikely events will occur if given enough time. Risk management and BCP are often mistakenly seen as overlapping practices. In fact these processes are so tightly tied together that such separation seems artificial. For example, the risk management process creates important inputs for the BCP (assets, impact assessments, cost estimates etc). Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the BCP process.

Risk Management and Internal Auditors

The 21st century internal auditors have the following vital areas of responsibility:

- Review operations, policies, and procedures
- Help ensure goals and objectives are met

- Understanding of “big picture” and diverse operations
- Make recommendations to improve economy and efficiency

The enhanced role of the internal auditor covers, *inter alia*,

- Risk management, control, and governance processes
 - Financial analysts
 - Risk evaluators
 - Improving operations, business performance
 - Supplying analyses, suggestions, and recommendations

Some Important Services Rendered by Internal Auditors

Risk Assurance

One of the primary roles of internal audit is risk assurance. Internal auditors identify all auditable activities and relevant risk factors, and assess their significance.

- Investigating
- Evaluating
- Identifying potential trouble spots
- Communicating
- Anticipating emerging issues
- Identifying opportunities

Internal Control Assessments

The internal auditor assess the ‘as –is’ internal control system within the organization and map it against a globally accepted ‘standard’ which is basically, an Internal Controls framework- COSO being the most widely used.

Training Material on Internal Audit

- Evaluate efficiency and effectiveness of controls
- Recommend new controls where needed – or discontinuing unnecessary controls
- Use of control frameworks (COSO, CoCo, Cadbury)
- Control self-assessment (CSA)

Specific Role of Internal Audit in Enterprise Risk Management

Internal auditors should recognize that there could be significant variations in techniques used by various entities for their risk management practices. The internal auditors:

- Obtain a document containing the enterprise risk management framework and accordingly ascertain that the process is both comprehensive and suitable for the nature of the organization.
- Research and review reference materials and background information on risk management methodologies as a basis to assess whether or not the process used by the organization is appropriate and represents best practices for the industry.
- Determine whether the risk management procedures are clearly understood by all key levels involved in the risk management process.
- Review corporate policies, board, and audit committee minutes to determine the organization's business strategies, risk management philosophy and methodology, appetite for risk, and acceptance of risks.
- Review previous risk evaluation reports by management, internal auditors, external auditors, and any other sources that may have issued such reports.

- Assist in planning the procedures in risk management framework based on his specialized knowledge of the business.
- Assist by examining, evaluating, reporting, and recommending improvements on the adequacy and effectiveness of management's risk processes.
- Ensure that early warning mechanism of disaster exists.
- Audit the risk management process across the entire entity.
- Assess whether the risk management framework has to be updated and whether any improvements in the ERM process are needed.
- Assess how well the risks identified by the management have been managed.
- Conduct interviews with line and executive management to determine business unit objectives, related risks, and management's risk mitigation and control monitoring activities.
- Participate in the monitoring and reporting activities in the risk management process.
- Provide training to the risk management committee and facilitate Risk-based work-shops.
- Assess the business continuity plan and ensure that a comprehensive disaster plan exists.
- Provide support in case of a negative impact on the business by assisting the business to recover.

Risk Identification Process: Internal Auditor's Role

The role would include:-

- Independently evaluating whether all probable risks have been identified and prioritized in the order of their significance.

Training Material on Internal Audit

- Ascertaining whether even events with a relatively low possibility of occurrence has been identified and considered if the impact of achieving an important objective is great.
- Ascertaining that the organization has adopted the appropriate techniques to assess the severity of the risks.
- Ascertaining that the management has used a combination of qualitative and quantitative techniques in risk assessment.

Risk Treatment Process: Internal Auditor's Role

The role would include:-

- Ascertaining that any system of risk treatment should be designed to bring anticipated risk likelihood and impact within tolerance level.
- Evaluating whether the risk response should ensure effective internal controls and adhere to applicable laws and regulations.

Risk Reporting Process: Internal Auditor's Role

The role includes:-

- Ascertaining that the reporting is both timely and effective.
- Ensuring that significant deficiencies discovered in the risk management process are clearly documented.

Risk Monitoring Process: Internal Auditor's Role

The role involves:-

- Assessing whether appropriate controls exist in the organization and that monitoring activities are progressing in an efficient manner.
- Evaluating focus on the effectiveness of the enterprise risk management.

Internal Audit Checklist for Risk Management

- 1) Has the management established entity-wise and activity wise objectives after considering associated risks and their implications?
- 2) Has the management communicated the objectives to all the employees?
- 3) Has the risk management plan been drawn in consistent with the objectives?
- 4) Have the concerned personnel understood the policies and procedures in risk management?
- 5) Have the key personnel understood the level of responsibility and accountability?
- 6) Is the mechanism adequate to identify risks from :
 - a) external sources
 - b) internal sources
- 7) Does the management select technique that fit its risk management process and does the entity develop risk identification capabilities.
- 8) Is information gathered pertinent and assimilated in a proper form?
- 9) Are the risk analysis and evaluation techniques effective?
- 10) Does the management consider additional risk that might result from a response selected to treat a risk?
- 11) In selecting a control technique does management consider how control activities co-relate?
- 12) Is the communication activity across the organization adequate?
- 13) Is the information provided timely, efficient and sufficient?
- 14) Is the follow-up action timely and appropriate?

Training Material on Internal Audit

- 15) Have the training workshops/seminars been effective?
- 16) Is the internal control system effective?
- 17) Is importance given to documentation including policy manuals, organization charts, operating instructions, documentation of evaluation process etc?
- 18) Is there a mechanism in place to identify changes that could affect achievement of objectives?
- 19) Are policies and procedures modified as and when necessary?
- 20) Is the competence of the personnel commensurate with their responsibilities?

Key Drivers for Developing Internal Audit Effectiveness for ERM include

- Respect and integrity throughout the organization.
- Clear, updated charter and adapts its activities to the needs of the organization.
- Teams with other internal and external resources.
- Provides leadership on issues of internal control, fraud, financial reporting, risk management, and corporate governance.
- Leverages technology.
- Uses a risk-based approach.
- Deploys best-available methodologies.
- Engages in continuous education and staff development.
- Consistently reevaluates its effectiveness.
- Provides support to the company's anti-fraud programs.
- Reports directly to the audit committee and maintains open communication with management.

Chapter-I.4

Sarbanes Oxley Act (SOX)– Milestone in the Perspective of Internal Audit

The Sarbanes-Oxley Act of 2002 was enacted on in July 2002, in USA, and commonly called SOX in response to a number of major corporate scandals such as Enron, Tyco International, Adelphia, Peregrine Systems and WorldCom. These hi-profile scandals, which cost investors billions of dollars when the share prices of the affected companies collapsed, shook public confidence in the nation's securities markets. Named after sponsors Senator Paul Sarbanes and Representative Michael G. Oxley, the Act was approved by the House by a vote of 423-3 and by the Senate 99-0. President George W. Bush signed it into law, stating it included "the most far-reaching reforms of American business practices since the time of Franklin D. Roosevelt."

The legislation establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. It does not apply to privately held companies. The Act contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law. Debate continues over the perceived benefits and costs of SOX. The Act establishes a new quasi-public agency, the Public Company Accounting Oversight Board, or PCAOB, which is charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies. The Act also covers critical issues such as:

- Auditor independence,
- Corporate governance,
- Corporate fraud responsibility,

Training Material on Internal Audit

- Penalties,
- Internal control assessment, and
- Enhanced financial disclosure.

A variety of complex factors created the conditions and culture in which a series of large corporate frauds occurred between 2000-2002. These frauds and others resulted in over U.S. \$500 billion in market value declines. The analysis of their complex and contentious root causes contributed to the passage of SOX in 2002. Specific contributing factors were:

- **Boardroom failures:** Boards of Directors, specifically Audit Committees, are charged with establishing oversight mechanisms for financial reporting in U.S. corporations on the behalf of investors. These scandals highlighted that some Board members either did not exercise their responsibilities or did not have the expertise to understand the complexities of the businesses. In many cases, Audit Committee members were not truly independent of management.
- **Securities industry conflicts of interest:** The roles of securities analysts, who make buy and sell recommendations on company stocks and bonds, and investment bankers, who help provide companies loans or handle mergers and acquisitions, provide opportunities for conflicts. Issuing a buy or sell recommendation on a stock while providing lucrative investment banking services creates at least the appearance of a conflict of interest.
- **Banking practices:** Lending to a firm sends signals to investors regarding the firm's risk. In the case of Enron, several major banks provided large loans to the company without understanding, or while ignoring, the risks of the company. Investors of these banks and their clients were hurt by such bad loans, resulting in large settlement payments by the banks. Others interpreted the willingness of banks to lend money to the company as an indication of its health and integrity, and were led to invest in Enron as a result. These investors were hurt as well.

- **Executive compensation:** Stock option and bonus practices, combined with volatility in stock prices for even small earnings "misses," resulted in pressures to manage earnings. Stock options were not treated as compensation expense by companies, encouraging this form of compensation. With a large stock-based bonus at risk, managers were pressured to meet their targets.

Sarbanes-Oxley contains 11 titles that describe specific mandates and requirements for financial reporting. Each title consists of several sections, as follows:

TITLE I -- "Public Company Accounting Oversight Board (PCAOB)"

Title I establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX. Title I consists of nine sections.

TITLE II -- "Auditor Independence"

Title II consists of nine sections, establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation policy, conflict of interest issues and auditor reporting requirements. Section 201 of this title restricts auditing companies from doing other kinds of business apart from auditing with the same clients.

TITLE III -- "Corporate Responsibility"

Title III mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of

Training Material on Internal Audit

corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance. For example, Section 302 implies that the company board (Chief Executive Officer, Chief Financial Officer) should certify and approve the integrity of their company financial reports quarterly. This helps establish accountability. Title III consists of eight sections.

TITLE IV -- "Enhanced Financial Disclosures"

Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.

TITLE V -- "Analyst Conflicts of Interest"

Title V consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

TITLE VI -- "Commission Resources and Authority"

Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions under which a person can be barred from practicing as a broker, adviser or dealer.

TITLE VII -- "Studies and Reports"

Title VII consists of five sections. These sections 701 to 705 are concerned with conducting research for enforcing actions against violations by the SEC registrants (companies) and auditors.

Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing and others to manipulate earnings and obfuscate true financial conditions.

TITLE VIII -- "Corporate and Criminal Fraud Accountability"

Title VIII consists of seven sections and it also referred to as the "Corporate and Criminal Fraud Act of 2002." It describes specific criminal penalties for fraud by manipulation, destruction or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.

TITLE IX -- "White Collar Crime Penalty Enhancement"

Title IX consists of two sections. This section is also called the "White Collar Crime Penalty Enhancement Act of 2002." This section increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

TITLE X -- "Corporate Tax Returns"

Title X consists of one section. Section 1001 states that the Chief Executive Officer should sign the company tax return.

TITLE XI -- "Corporate Fraud Accountability"

Title XI consists of seven sections. Section 1101 recommends a name for this title as "Corporate Fraud Accountability Act of 2002" . It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments.

Major Sections and their Implications

Section 302: Internal Control Certifications

Under Sarbanes-Oxley, two separate certification sections came into effect—one civil and the other criminal. Section 302- (civil provision); Section 906- (criminal provision). Section 302 of the Act mandates a set of internal procedures designed to ensure accurate financial disclosure. The signing officers must certify that they are “responsible for establishing and maintaining internal controls” and “have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared.” The officers must “have evaluated the effectiveness of the company’s internal controls as of a date **within 90 days prior to the report**” and “have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.”

SOX Section 404: Assessment of Internal Control

The most contentious aspect of SOX is Section 404, which requires management and the external auditor to report on the adequacy of the company's internal control over financial reporting (ICFR). This is the most demanding aspect of the legislation for companies to implement, as documenting and testing important financial manual and automated controls requires enormous effort.

Under Section 404 of the Act, management is required to produce an “internal control report” as part of each annual Exchange Act report. The report must affirm “the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.” The report must also “contain an assessment, as of the end of the most recent fiscal year of the company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.” To do this, managers are generally adopting an internal control framework such as that described in COSO.

Both management and the external auditor are responsible for performing their assessment in the context of a top-down risk

assessment, which requires management to base both the scope of its assessment and evidence gathered on risk. Both the PCAOB and SEC recently issued guidance on this topic to help alleviate the significant costs of compliance and better focus the assessment on the most critical risk areas.

The recently released **Auditing Standard No. 5 of the Public Company Accounting Oversight Board (PCAOB)**, which superseded Auditing Standard No 2. has the following key requirements for the external auditor:

- Assess both the design and operating effectiveness of selected internal controls related to significant accounts and relevant assertions, in the context of material misstatement risks;
- Understand the flow of transactions, including IT aspects, sufficiently to identify points at which a misstatement could arise;
- Evaluate company-level (entity-level) controls, which correspond to the components of the COSO framework;
- Perform a fraud risk assessment;
- Evaluate controls designed to prevent or detect fraud, including management override of controls;
- Evaluate controls over the period-end financial reporting process;
- Scale the assessment based on the size and complexity of the company;
- Rely on management's work based on factors such as competency, objectivity, and risk;
- Evaluate controls over the safeguarding of assets; and
- Conclude on the adequacy of internal control over financial reporting.

Training Material on Internal Audit

After the release of this guidance, the SEC required smaller public companies to comply with SOX Section 404, companies with year ends after December 15, 2007. Smaller public companies performing their first management assessment under Sarbanes-Oxley Section 404 may have found their first year of compliance after December 15, 2007 particularly challenging.

SOX Section 802 Criminal Penalties for Violation of SOX

Section 802(a) of the SOX, states:

“Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.”

SOX Section 1107 Criminal Penalties for Retaliation Against Whistleblowers

Section 1107 of the SOX states:

“Whoever knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any federal offence, shall be fined under this title, imprisoned not more than 10 years, or both.”

Implications for Executives

CFO's – Required Action

- Implement, document, and test internal controls over processes that contribute to the financial statements (Section 302 and 404)

- Certify, under criminal penalty, that these controls work

Hurdles

- Currently, control testing is a highly manual, expensive, and time consuming
- Control monitoring on any regular basis is rarely done

External Auditors – Required Action

- Review the corporate documentation
- Re-test the controls to confirm management's assessment
- Issues opinions and report them to the public

Hurdles

- Typically, several companies per month had to report these embarrassing violations or failures

Benefits of SOX

- Increased confidence of CEO/CFO in meeting reporting requirements
- Improved coordination of Company Management Team
- Improved and clarified Corporate Governance process
- Systematized process for early identification of business risks/ whistle blowing issues/incident management
- Systematized approach to dealing with change (i.e., transactions, personnel, accounting principles, internal controls and operating procedures)
- Increased operational effectiveness

Implications for Internal Auditor's Understanding

- Understand that SOX is the model for legislative initiatives aimed at both public and private companies in a number of states.
- Maintain a strong and independent audit committee (where used).
- Keep any arrangements for the auditor to provide non-audit services independent of audit services.
- Ensure executives understand the financial, compliance, and other external information reporting.
- Establish, maintain, and document significant financial and compliance controls.
- Maintain and archive all appropriate entity records.
- Remember SOX is the benchmark against which every company's financial and corporate governance practices will be measured.

Conclusion - SOX has brought in a sea-change in corporate disclosures, accountability and governance process but with its own share of misses and pitfalls. A concerted effort, however, is still required by management, auditors, consultants and regulatory bodies to reap the full benefits of the provisions of this epoch-making piece of legislation.

Chapter-I.5

Discussions on Revised Clause 49

Clause 49 of the SEBI guidelines on Corporate Governance as amended on 25th October, 2004 has made major changes in the :

- definition of independent directors,
- strengthening the responsibilities of audit committees,
- improving quality of financial disclosures, including those relating to related party transactions and proceeds from public/ rights/ preferential issues,
- requiring Boards to adopt formal code of conduct,
- requiring CEO/CFO certification of financial statements and for improving disclosures to shareholders.
- certain non-mandatory clauses like whistle blower policy and restriction of the term of independent directors have also been included.

The term '*Clause 49*' refers to clause number 49 of the Listing Agreement between a company and the stock exchanges on which it is listed (the Listing Agreement is identical for all Indian stock exchanges, including the NSE and BSE). Clause 49, when it was first added, was intended to introduce basic corporate governance practices in Indian companies and brought in a number of key changes in governance and disclosures. It specified the minimum number of independent directors required on the board of a company. The setting up of an Audit committee, and a Shareholders' Grievance committee, among others, were made mandatory as were the Management's Discussion and Analysis (MDandA) section and the Report on Corporate Governance in the Annual Report, and disclosures of fees paid to non-executive directors. A limit was placed on the number of committees that a director could serve on. In late 2002, SEBI

Training Material on Internal Audit

constituted the Narayana Murthy Committee to assess the adequacy of current corporate governance practices and to suggest improvements. Based on the recommendations of this committee, **SEBI issued a modified Clause 49 on October 29, 2004 (the 'revised Clause 49') which came into operation on January 1, 2006.**

SEBI Circulars on Clause 49 are as –

S. No	Circular No	Date
1	SMDRP/POLICY/CIR-10/2000	February 21,2000
2	SMDRP/POLICY/CIR-13/2000	March 09, 2000
3	SMDRP/POLICY/CIR-42/2000	September12, 2000
4	SMDRP/POLICY/ CIR- 03/01	January 22, 2001
5	SMDRP/POLICY/ CIR- 19/01	March 16,2001
6	SMDRP/POLICY/ CIR- 53/01	December 31,2001
7	SEBI/MRD/SE/31/2003/26/0	August 26, 2003

Details of recent Amendments –

S. No	Circular No	Date
1	SEBI/CFD/DIL/CG/1/2004/12/10	October 29,2004
2	SEBI/CFD/DIL/CG/1/2005/29/3	March 29, 2005
3	SEBI/CFD/DIL/CG/1/2006/13/1	January 13, 2006

The revised Clause 49 has suitably pushed forward the original intent of protecting the interests of investors through enhanced governance practices and disclosures.

Five broad themes predominate. These are as –

- The independence criteria for directors have been clarified.

Discussions on Revised Clause 49

- The roles and responsibilities of the board have been enhanced.
- The quality and quantity of disclosures have improved.
- The roles and responsibilities of the audit committee in all matters relating to internal controls and financial reporting have been consolidated, and
- The accountability of top management—specifically the CEO and CFO—has been enhanced.

Within each of these areas, the revised Clause 49 moves further into the realm of global best practices.

The major new provisions included in the Clause 49 are:

- 1) The board will lay down a code of conduct for all board members and senior management of the company to compulsorily follow.
- 2) The CEO and CFO will certify the financial statements and cash flow statements of the company.
- 3) At least one independent director of the holding company will be a member of the board of a material non-listed subsidiary.
- 4) The audit committee of the listed company shall review the financial statements of the unlisted subsidiary, in particular its investments.
- 5) If while preparing financial statements, the company follows a treatment that is different from that prescribed in the accounting standards, it must disclose this in the financial statements and the management should also provide an explanation for doing so in the corporate governance report of the annual report.
- 6) The company will have to lay down procedures for informing the board members about the risk management and minimisation procedures.

- 7) Where money is raised through public issues, rights issues etc., the company will have to disclose the uses/applications of funds according to major categories (capital expenditure, working capital, marketing costs etc) as part of quarterly disclosure of financial statements. Further, on an annual basis, the company will prepare a statement of funds utilised for purposes other than those specified in the offer document/prospectus and place it before the audit committee.
- 8) The company will have to publish its criteria for making its payments to non-executive directors in its annual report.

Who is an Independent Director?

The definition of independent directors as given in the revised clause 49 is an inclusive definition, which defines independent directors as follows:

"For the purpose of this clause the expression 'independent directors' means directors who apart from receiving director's remuneration, do not have any other material pecuniary relationship or transactions with the company, its promoters, its management or its subsidiaries, which in judgment of the board may affect independence of judgment of the directors."

The definition of the term 'Independent Directors' has been amended to mean a Non-Executive Director who:

- Does not have a pecuniary relationship with the company, its promoters, senior management or affiliate companies.
- Is not related to promoters or the senior management.
- Has not been an executive with the company in the immediately three preceding financial years.
- Is not a partner or executive of the auditors/lawyers/consultants of the company.
- Is not a supplier, service provider or customer of the company.

- Does not hold 2 per cent or more of the shares of the company.
- 9) Further, there is certain minimum information that is required to be made available to the members of the board prior to the board meeting **which ranges from annual operating plans and budgets to labour problems.**

In India specifically, the *revised Clause 49* of the Listing Agreement has proposed far reaching changes across the entire spectrum of governance activities including;

- Board composition and procedure
- Audit committee responsibilities
- Subsidiary companies oversight
- Risk management
- CEO/CFO certification of financial statements and internal controls
- Legal compliance monitoring; and
- Other disclosures

Many of these welcome requirements, particularly the risk management and internal control evaluation, are aimed at rapidly moving Indian companies towards a process and system driven organizations. To ensure success and sustainability, it requires a significant degree of management oversight, consultative support, regulatory body involvement and overall effort by organizations.

Chapter-I.6

Audit Committee and Role of Internal Audit

Today's organizations operate in a multi-dimensional, multi-disciplinary, probabilistic, adaptive and dynamic business environment. While the complexity of operations has multiplied, the aspects of risk management, harnessing IT best practices and superior corporate governance codes are the keys to success and sustainability. The role of the Audit Committee is indispensable in the overall framework of corporate governance, oversight of the entity's operations and in the functioning of a process-driven organization.

Some of the vital roles and responsibilities of Audit Committees are discussed; essentially they embody the global best-in-class practices:

- **Developing enterprise-wide risk management and oversight** - Risk management, and the role of the audit committee and board in its oversight are rightly considered to be a prime issue, given the importance of risk management to the company's financial reporting and disclosure processes, the audit committee can play the role of a catalyst in identifying lapses and gaps in the company's risk management processes, and helping in coordination of the oversight activities of the board in this area. Audit committee needs to ensure that the activities of senior management set a clear, unambiguous and consistent tone in this regard.
- **Championing a shared vision for internal audit** - The audit committee define the level of involvement of internal audit in risk management and operational audits while maintaining the requisite focus on internal controls and financial audits / review. Issues like adequate resourcing and skill sets for the internal audit job , in the light of today's tight talent pool—are important areas of focus. A fresh look is

needed to reinforce the independence of the internal auditor and its accountability to the audit committee.

- **Expediting IFRS and other key financial reporting issues-** From fair value accounting, to the convergence of IFRS, including critical accounting policies, judgments, and estimates, audit committee's focus and challenge is to understand the implications of important financial reporting issues and developments affecting the entity. The audit committee needs to urge the management to cover *one* key financial reporting issue or development at each audit committee meeting. The external auditors may then be asked to comment on how the item is audited. The external audit engagement partner may be requested to provide important information on a real-time basis on areas of concern before they become major problems. Informal communications with the engagement Partner are also critical to establishing a solid working relationship with the auditor.
- **Supporting the CFO and the finance team -** Audit committee support of the CFO and the finance organization has become more critical, in areas like succession planning, resources and infrastructure, evaluations for the CFO and finance team etc.
- **Monitoring management's disclosure committee -** Audit committees need to monitor closely the activities of the disclosure committee, ensuring that the communications and reports are adequate.
- **Crisis Management -** Allegations and / or media coverage of financial irregularities, creative accounting practices, lack of financial discipline etc highlights the importance of having a formal plan in place before a crisis occurs—including the ability to implement a credible, objective and independent investigation on a timely basis.
- **Communicating to the board about the audit committee's activities -** The audit committee's communication with the board is one of the important foundations for effective oversight. This will ensure that the

Training Material on Internal Audit

central role of the audit committee in the oversight of financial reporting, disclosures, internal controls, risk management, and compliance are brought to its logical and meaningful conclusion.

- **Self assessment of performance** - Last but not the least, effective and productive annual self-assessments are essential. After securing the concurrence of all committee members towards making a commitment for the self-assessment process, the next steps are to engage the necessary resources and expertise to formulate a self-assessment process that works for the audit committee and finally to follow through and implement on a sustained basis.

The above measures are indicators of excellence for the audit committee's performance and will pave the way for increased effectiveness, superior oversight and structuring a risk-intelligent organisation.

Fraud Risk Management - Role of Internal Audit

Historical Perspectives

Enron

In the case of Enron, several major banks provided large loans to the company without understanding, or while ignoring, the risks of the company. Investors of these banks and their clients were hurt by such bad loans, resulting in large settlement payments by the banks. Others interpreted the willingness of banks to lend money to the company as an indication of its health and integrity, and were led to invest in Enron as a result. These investors were hurt as well.

In 2001, Enron admitted to inflating profits leading to:

- Thousands of jobs and millions of dollars in pensions lost
- The collapse of Enron's auditors, Arthur Anderson

Worldcom and Tyco

- In 2002, WorldCom revealed an \$11bn accounting fraud leading to:
 - Shareholder losses around £94 billion.
 - 25 years in prison for Bernard J Ebbers, former Chief Executive.
- In 2002, Tyco senior executives were discovered to have stolen \$600m from the company leading to:
 - Up to 25 years each in prison.
- Total personal fines totalling \$134 million.

Training Material on Internal Audit

A recent study conducted in US has shown - 49% of Investors and 29% of Executives claim corporate scandals in recent years as one of the top reasons for increased importance of corporate responsibility. Corporate fraud has of late, been the focal point of attention in Board rooms across the world, in the aftermath of financial scandals in Enron, Tyco, Adelphia, Worldcom and others. The Sarbanes Oxley Act (SOX) and the Foreign Corrupt Practices Act (FCPA) are two of the more prominent legislation against the menace of fraud.

Major types of fraud are as under:

- Management Fraud
- Employee Fraud
- External Fraud
- Combination Fraud

Some other categories of fraud can be:

- Misappropriation of Assets – forgery, theft, embezzlement, falsification of timesheets and payroll, over-stated expenses.
- Fraudulent Financial Reporting (FFR)- Window dressing, improper revenue recognition, overstatement of assets, understatement of liabilities.
- Expenditures and Liabilities for improper purposes – Bribery, Kick-backs.
- Fraudulently obtained revenue and assets.

For all types of frauds, the basic tenet is the existence of the fraud triangle. There must be an Incentive for the fraud, a suitable Opportunity to perpetrate the fraud and lastly, a mental attitude to perpetrate fraud.

The underlying features in many types of fraud is – overriding of internal control. In cases of Fraudulent Financial Reporting (FFR), one of the potent factors is – unsystematic basis for revenue recognition. Some of the areas vulnerable to fraud are Purchases,

Sales, Inventory and Payroll. Several types of theft / embezzlement have been observed, such as:

- Expense Account Fraud
- Theft of Assets
- Charging Personal Expenses to the Corporate Account
- Diverting Transactions to Concealed Related Parties
- Conspiracy to Pay Fictitious Fees
- Theft of Information, Trade Secrets, Trade Marks

Employee fraud constitutes a large chunk of cases of reported fraud. Reasons of employee fraud could be due to personal debts, changing lifestyle and rise of consumerism, employee layoffs, inconsistent promotion and disgruntlement, large cash in hand and easy access to company assets. In the case of projects and large contracts, there are chances of kickbacks and secret commissions - Offering or accepting any reward advantage or benefit for doing any act relating to business, false invoices and false representations.

The consequences of fraud are devastating – it affects viability and profitability, results in reputational damage and public embarrassment, financial losses, loss of key staff and customers, loss of management time, loss of sensitive intellectual property, Regulatory fines and penalties, legal and investigative costs and consequential loss of business.

What are red flags – These are warning signs that frauds have occurred. Such signs must be proactive, not reactive. Persons raising red flags are known as ‘whistleblowers’ – they must always be conscious of the unusual or the out of place. Some salient signs of red flags are as:

- Infighting among Top Management
- Inconsistent and Surprising Cash Flow Deficiencies
- Employee with Unexplained Lavish Lifestyle

Training Material on Internal Audit

- Frequent Complaints from Customers, Suppliers etc
- Low Morale and Motivation among Employees
- Under staffed Accounting Departments

Some Red flags or warning signs or fraud-indicators associated with employee fraud:

- No or little segregation of duties
- Established controls or procedures are not followed
- Minimal monitoring of employee performance
- Employee never takes vacations
- High Employee Turnover
- Employees feel they are “owed something”
- No Corporate “conflict of interest” policies
- Code of ethics nonexistent or not followed

Typical aspects of a Fraud Deterrence and Prevention approach should include:

- Establishing the right culture and ‘tone at the top’
- Establishing a whistle-blowing and anti-fraud policy
- Developing a Code of Conduct and Integrity helpline
- Identify risks and implement effective Internal controls
- Internal Audits with special ‘Surprise Audits’
- Planning for the worst (DRP)
- Recruiting the right people with adequate background checks
- Regular fraud substantive audits

- Deploying proper IT Security
- System of Vendor Appraisal, Receiving Report and Physical checking at entry points
- System of segregation and rotation of duties, employee background checks etc

Internal Auditors Role in Fraud Prevention

1. Internal auditors are responsible for helping *deter fraud* by examining and evaluating the *adequacy and the effectiveness of controls*, along with the *extent of the potential exposure and risk in the various segments* of the entity's operations.
2. Internal auditors need to consider the following –
 - Fostering control consciousness
 - Appropriate authorization policies
 - Practical and working policies, practices, procedures, reports, and other mechanisms
 - MIS and communication channels

The best defense against fraud are strong internal controls, fraud risk awareness and suitable anti-fraud programs. The Quality of anti-fraud strategy within the organization and the responsibility for managing fraud risk should be well defined. There should be presence of clear channels for reporting suspicions of fraud , adequate protection offered to whistle-blowers, effectiveness of recruitment screening procedures and last but not the least – the appropriate tone at the top.

MODULE - II

STANDARDS ON INTERNAL AUDIT

Internal audit is an independent appraisal involving specialized application of techniques of auditing in accordance with the specific needs of an enterprise. The nature and scope of internal audit depends upon the requirements of an enterprise. It is a systematic evaluation of risk management, control and governance processes particularly with reference to:

- Safeguarding of assets
- Compliance with laws, regulations and contracts as well as policies laid down by the management
- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations
- Accomplishment of objectives and goals of the organization through ethical and effective governance

The Institute of Chartered Accountants of India constituted the “Committee on Internal Audit” on 5th February 2004. The Council, at its 282nd meeting held in November 2008, had renamed the Committee on Internal Audit as “Internal Audit Standards Board”. The primary mission of the Board is to enable its members to provide more effective and efficient value added services relating to internal audit to the industry and others by issuing Standards on Internal Audit, Guidance Notes and Industry Specific Technical Guides.

The following definition of internal audit, as contained in the Preface to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India, amply reflects the current thinking as to what is an internal audit:

“3. Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system.”

It is, however, pertinent to note that variations in propositions do not change the basic philosophy of collecting and evaluating evidence and formulating an opinion; what undergoes a change is the approach, the tools and the techniques used. Internal audit is, therefore, an important tool in the hands of the management to help improve its decision making process. The growing importance of internal audit to good governance can be appreciated from the spate of legal and regulatory requirements world over, directly or indirectly necessitating the need for internal help management to rope in the services of internal audit to help in improving the former's efficiency in running an enterprise. However, before discussing how internal audit can help management in that respect and the drivers of an efficient and effective internal audit, it is essential to understand the various stages of evolution of internal audit over time.

Preface to Standards on Internal Audit

The Preface to Standards on Internal Audit is an important document, which gives an insight into Committee on Internal Audit (presently known as Internal Audit Standards Board). It deals with aspects like scope and functions of the Committee on Internal Audit, scope of Standards on Internal Audit and Guidance Notes on Internal Audit and their status being mandatory or recommendatory in nature, as also the implications in case of departures from the Standards on Internal Audit, the basic procedures for issuing the Standards and Guidance Note on Internal Audit and the date of coming into force of the particular Standard on Internal Audit.

Preface to Standards on Internal Audit issued by the Institute of Chartered Accountants of India is given in **Appendix I**.

Framework for Standards on Internal Audit

Internal Audit Standards Board has issued the Framework for Standards on Internal Audit which provides a frame of reference for the internal audit standards being issued by the Institute. The objective of the Framework is to promote the

professionalism in the internal audit activity. The Framework comprises of four components viz the Code of Conduct, the Competence Framework, the Body of Standards and the Technical Guidance.

Framework for Standards on Internal Audit issued by the Institute of Chartered Accountants of India is given in **Appendix II**.

Basic Principles Governing an Internal Audit

Like any other profession, the profession of internal audit also is based on a certain fundamental principles, which constitute the life and blood of this profession. Standard on Internal Audit (SIA) 2, *Basic Principles Governing Internal Audit*, had also been issued by the Institute of Chartered Accountants of India. The purpose of this Standard on Internal Audit (SIA) is to establish standards and provide guidance on the general principles governing internal audit. This Standard explains the principles, namely, integrity, objectivity and independence, confidentiality, due professional care, skills and competence, work performed by others, documentation, planning, Evidence and reporting which governs the internal auditor's professional responsibilities. These principles have been discussed in the following paragraphs:

Integrity, Objectivity and Independence

The internal auditor should be straight forward, honest and sincere in his approaching to the assignment, keeping free of any bias that may override/compromise his integrity and objectivity. The internal auditor should also be impartial and free of any interest that may be regarded as incompatible to integrity and objectivity and inform his supervisors of any personal or external factors that actually do or are likely to impede his independence and objectivity so that necessary remedial action may be taken.

Confidentiality

The internal auditor, in the course of his work, invariably comes across information that is confidential and/ or critical to the working of the entity. The internal auditor should respect the confidentiality of such information and should not disclose the same to a third party without the specific authority or unless there is a legal or professional duty to do so. The internal auditor should, therefore, ensure that there are adequate policies and mechanisms to protect the confidentiality of the information.

Due Professional Care, Skills and Competence

Performance of the audit and preparation of the report require due professional care by persons who have adequate training, experience and competence in auditing. Development of audit skills may be achieved through training courses. Much of staff development results from on the job training where experienced auditors assist in the training of new, less experienced internal staff. Each internal auditor is responsible for continuing his education in order to maintain his proficiency.

Internal auditors should also take reasonable professional care in specifying evidence required, in gathering and evaluating that evidence and in reporting the findings. They need to remain alert to the instances that could indicate errors, fraud, etc.

Planning

Adequate planning for every audit should cover all material areas. The audit working papers should incorporate documentary evidence of audit planning in the form of an audit plan, setting out the objectives and scope of an audit and the techniques and resources to be used by an internal auditor. Plans may be revised as required in the course of the audit.

Delegation and Supervision

Internal auditor would invariably require delegating work to assistants. At times, services of an expert might also be sought. The internal auditor would, however, continue to be responsible

for his opinion on the activities being subject to internal audit or his findings. The internal auditor should carefully direct, supervise and review the work delegated to assistants. The amount of supervision required depends on the skill and experience of the assistant on the job. The supervisory role of the internal auditor includes:

- Providing suitable instructions for the audit.
- Approving or recommending the approval of the audit plan.
- Ensuring that the audit program is completed.
- Ensuring that working papers adequately support the audit findings, conclusions and reports.
- Ensuring that the reports are unambiguous, accurate and concise.
- Ensuring that the audit objectives have been met.

Evaluation of Internal Control

Internal auditors should systematically evaluate the nature of operations and system of internal controls in the departments being audited to determine the nature, extent and timing of audit procedures. Internal controls of an organization comprise the plan of organization and methods adopted to safeguard assets, comply with laws, ensure the completeness and correctness of data, promote efficiency and encourage adherence to management policies. It is important that a review of an internal control system be directed primarily towards those controls that have an important bearing on the reliability of the system (i.e., key controls).

Evidence

The internal auditor should obtain all the evidence considered necessary for the expression of an informed opinion. Professional judgment is needed to determine the nature and amount of evidence required. In this regard, the internal auditor should consider:

- The item under consideration;

Training Material on Internal Audit

- Materiality of possible errors;
- Degree of risk of error; and
- Probability of the error occurring.

Work Papers

The internal auditor should document matters that are important in providing evidence to his opinion or the findings. Advantages of having sufficient and properly maintained work papers include the following:

- Assistance in the performance of the audit.
- Providing record of work done.
- Forming basis of the auditor's observations/ findings in his report.
- Providing information for the report.
- Aiding the review and evaluation of the work done.
- Aiding cross referencing between audit evidence and decision taken by the internal auditor.
- Providing evidence that the internal audit was carried out in accordance with the requirements of the relevant pronouncements of the Institute of Chartered Accountants of India.

Standard on Internal Audit (SIA) 2, *Basic Principles Governing Internal Audit* issued by the Institute of Chartered Accountants of India is given in **Appendix IV**.

Planning an Internal Audit

Planning is one of the basic principles governing internal audit. Adequate planning ensures that appropriate attention is devoted to significant areas of audit, potential problems are identified, and that the skills and time of the staff are appropriately utilised. Planning also ensures that the work is carried out in accordance with the applicable pronouncements

of the Institute of Chartered Accountants of India. Planning should also be based on the knowledge of the entity's business. Standard on Internal Audit (SIA) 1, *Planning an Internal Audit* was also issued by the Institute of Chartered Accountants of India. The basic objective of the SIA is to establish standards and provide guidance in respect of planning an Internal and helping in achieving the objectives of an Internal Audit function. The SIA 1 is given in **Appendix III**. This SIA gives an insight into the objectives of the planning. It provides knowledge about the factors affecting the planning process. It deals with the scope of the planning and planning process.

Documentation

Adequate documents act as basis for the planning and performing the internal audit. Documents provide the evidence of the work of the internal auditor. The Institute of Chartered Accountants of India had also issued the Standard on Internal Audit (SIA) 3, *Documentation*. The purpose of this Standard on Internal Audit is to establish Standards and provide guidance on the documentation requirements in an internal audit. This Standard provides guidance regarding the form and content of the internal audit documentation, detention and retention of the same and identification of the preparer and reviewer. The SIA 3 is given in **Appendix V**.

Reporting

Reporting is a formal opinion or disclaimer thereof, issued by the internal auditor as a result of evaluations made by him as per the terms of the engagement. The Institute of Chartered Accountants of India has also issued the Standard on Internal Audit (SIA) 4, *Reporting*. The purpose of the Standard on Internal Audit (SIA) 4, *Reporting* is to establish standards on the form and content of the internal auditor's report issued as a result of the internal audit performed by an internal auditor of the systems, processes, controls including the items of financial statements of an entity. This SIA describes the basic elements of an internal audit report such as opening, objectives, scope paragraphs, and executive summary. This SIA also deals with the different stages of communication and discussion of the

report and describes the reporting responsibilities of the internal auditor when there is a limitation on the scope. The Standard also lays down the reporting responsibilities of the internal auditor when there is restriction on usage and circulation of the report. The SIA 4 is given in **Appendix VI**.

Sampling

Sampling is that part of statistical practice concerned with the selection of individual observations intended to yield some knowledge about the audit population, especially for the purpose of statistical inference. The Institute of Chartered Accountants of India had also issued the Standard on Internal Audit (SIA) 5, *Sampling*. The Standard on Internal Audit (SIA) 5, *Sampling* provides the guidance regarding the design and selection of an audit sample and also on the use of the audit sampling in the internal audit engagements. This SIA also deals with the evaluation of the sample results. This Standard also provide guidance on the use of sampling in risk assessment procedures and tests of controls performed by the internal auditor to obtain an understanding of the entity, business and its environment, including mechanism of its internal control. The areas covered by the SIA include design of sample, tolerable and expected error, selection of sample, evaluation of sample results, analysis of errors in the sample, projection of errors, reassessing sampling risk. This also describes the internal auditor's documentation requirements in the context of the sampling. The SIA 5 is given in **Appendix VII**.

Analytical Procedures

Analytical Procedures is the skill which help an auditor understanding the client business and changes in the business, to identify potential risk arrears. The Institute of Chartered Accountants of India had also issued the Standard on Internal Audit (SIA) 6, *Analytical Procedures*. The Standard on Internal Audit (SIA) 6, *Analytical Procedures* provides the guidance regarding the application of analytical procedures during internal audit. The SIA deals with the aspects such as, the nature and purpose of analytical procedures, analytical procedures as risk assessment procedures and in planning the

internal audit, analytical procedures as substantive procedures, analytical procedures in the overall review at the end of the internal audit, extent of reliance on analytical procedures and investigating unusual items or trends. The SIA 6 is given in **Appendix VIII**.

Quality Assurance in the Internal Audit

Quality assurance is a standard for meeting the client requirements. It documents how an Internal Auditor will meet the requirements of a client or customer in a systematic, reliable fashion. It shows an Internal Auditor commitment to delivering quality products and services to the client. The Institute of Chartered Accountants of India had also issued the Standard on Internal Audit 7, *Quality Assurance in Internal Audit*. The Standard on Internal Audit (SIA) 7, *Quality Assurance in Internal Audit* establishes standards and provide guidance regarding quality assurance in internal audit. A system for assuring the quality in internal audit should provide reasonable assurance that the internal auditors comply with professional standards, regulatory and legal requirements so that the reports issued by them are appropriate in the circumstances. This Standard provide the guidance to the person entrusted with the responsibility for the quality of the internal audit whether in-house internal audit or a firm carrying out internal audit. This Standard also provides the extensive knowledge about the internal quality reviews, external quality reviews and communicating the results thereof. The SIA 7 is given in **Appendix IX**.

Terms of Internal Audit Engagement

The Terms of engagement defines the scope, authority, responsibilities, confidentiality, limitation and compensation of the internal auditors. Terms of Internal Audit Engagement lay down clarity between the internal auditors and the users of their services for inculcating professionalism and avoiding misunderstanding as to any aspect of the engagement. This Standard on Internal Audit (SIA) 8, *Terms of Internal Audit Engagement* provides guidance in respect of terms of engagement of the internal audit activity whether carried out in house or by an external agency. This SIA

Training Material on Internal Audit

describes the elements of the terms of engagement viz, scope, responsibility, authority, confidential, limitations, reporting, compensation and compliance with Standards. The SIA 8 is given in **Appendix X**.

APPENDIX I

**PREFACE TO THE STANDARDS
ON INTERNAL AUDIT¹**

CONTENTS

	Paragraph(s)
Formation of the Committee on Internal Audit	1
Scope and Functions of the Committee on Internal Audit	2
Scope of the Standards on Internal Audit	3
Procedure for Issuing the Standards on Internal Audit	4
Procedure for Issuing the Guidance Notes on Internal Audit	5
Compliance with the Standards and Guidance Notes on Internal Audit	6
Effective Date	7

¹ The original Preface to the Standards on Internal Audit was issued in November, 2004 and revised in July, 2007. The revised Preface has also been published in the August 2007 issue of *The Chartered Accountant*.

1. Formation of the Committee on Internal Audit

- 1.1 The Institute of Chartered Accountants of India constituted the “Committee for Internal Audit (CIA)” on 5th February 2004. At its 245th meeting held on November 29, 30 and December 1, 2005, the Council of the Institute of Chartered Accountants of India changed the nomenclature of the “Committee *for* Internal Audit” to “Committee *on* Internal Audit”.

2. Scope and Functions of the Committee on Internal Audit

- 2.1 A large number of the members of the Institute are involved in carrying out internal audit engagements. The Institute has, from time to time, issued general and industry specific guidelines on internal audit practices for the guidance of the members. The main function of the Committee on Internal Audit is to review the existing internal audit practices in India and to develop Standards on Internal Audit (SIAs). The SIAs aim to codify the best practices in the area of internal audit and also serve to provide a benchmark of the performance of the internal audit services. The SIAs are issued under the authority of the Council of the Institute.
- 2.2 While formulating the SIAs, the Committee will take into consideration the applicable laws, customs, usages and business environment and generally accepted auditing practices in India. The Committee may also, where it considers appropriate, take into consideration the international practices in the area of internal audit, to the extent they are relevant to the conditions existing in India.
- 2.3 The Committee on Internal Audit will also develop Guidance Notes on internal audit, including those on issues arising from the Standards on Internal Audit. These Guidance Notes will be issued under the authority of the Council of the Institute.
- 2.4 The Committee on Internal Audit will also formulate Clarifications on issues arising from SIAs. These

Clarifications will also be issued under the authority of the Council of the Institute.

3. Scope of the Standards on Internal Audit

- 3.1 The Standards on Internal Audit shall apply whenever an internal audit is carried out. Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system. Internal audit, therefore, provides assurance that there is transparency in reporting, as a part of good governance.

4. Procedure for Issuing the Standards on Internal Audit

Broadly, the following procedure will be adopted for issuing Standards on Internal Audit.

- 4.1 The Committee on Internal Audit will identify the broad areas in which the SIAs need to be formulated and the priority in regard to selection thereof.
- 4.2 In the preparation of the SIAs, the Committee will be assisted by Study Groups constituted to consider specific subjects. In the formation of the Study Groups, provision shall be made for participation of a cross section of members of the Institute. In situations considered necessary, the Committee may also consider having an expert on such Study Groups, subject to such terms and conditions, as may be finalised by the Committee. The expert need not necessarily be a member of the Institute of Chartered Accountants of India. The Study Group will be responsible for preparing the draft of the Standard.
- 4.3 The above mentioned draft Standard would be considered by the Committee. On the basis of the deliberations of the Committee on the draft Standard, an Exposure Draft of the proposed Standard will be prepared by the Committee and issued for comments by the members of the Institute. The

Exposure Draft will also be open for comments by non-members, including the regulators and other such bodies as well as general public.

- 4.4 The above mentioned Exposure Draft will be published in the Journal of the Institute and will also be hosted on the website of the Institute under appropriate head.
- 4.5 The Exposure Draft will normally remain open for comments for a period of at least sixty days from the date of issuance.
- 4.6 The above mentioned Exposure Draft will be circulated to all the Council members, Past Presidents, Regional Councils, Branches and CPE Study Circles of the Institute for their comments. The Exposure Draft will also be circulated to the following bodies, as may be necessary on a case to case basis, for their comments:
 - i. The Ministry of Corporate Affairs.
 - ii. The Reserve Bank of India.
 - iii. The Securities and Exchange Board of India.
 - iv. The Insurance Regulatory and Development Authority.
 - v. The Comptroller and Auditor General of India.
 - vi. The Central Board of Direct Taxes.
 - vii. The Institute of Cost and Works Accountants of India.
 - viii. The Institute of Company Secretaries of India.
 - ix. The Associated Chambers of Commerce and Industry.
 - x. The Federation of Indian Chambers of Commerce and Industry.
 - xi. The Confederation of Indian Industry.
 - xii. The Indian Banks' Association.
 - xiii. The Foreign Exchange Dealers' Association of India.

- xiv. The Standing Conference of Public Enterprises.
- xv. All recognised Stock Exchanges in India.
- xvi. The Competition Commission of India.
- xvii. The National Bank for Agricultural and Rural Development.
- xviii. The Controller General of Accounts.
- xix. The Ministry of Finance – Insurance and Banking Divisions.
- xx. The Indian Institute of Management - Ahmedabad, Bangalore, Kolkata, Indore, Kochi and Lucknow.
- xxi. The Central Registrar of Cooperative Societies, Government of India.
- xxii. The Bombay Mercantile Association.

The Committee may, however, in addition to the bodies listed above, circulate the Exposure Draft for comments to such other bodies also, as considered appropriate by it.

- 4.7 After taking into consideration the comments received on the Exposure Draft, the draft of the proposed Standard will be finalised by the Committee and submitted for the consideration of the Council of the Institute.
- 4.8 The Council of the Institute will consider the final draft of the proposed Standard on Internal Audit and if necessary, modify the same in consultation with the Committee on Internal Audit. The SIA will then be issued under the authority of the Council of the Institute.
- 4.9 For a substantive revision of a Standard on Internal Audit, the procedure followed for formulation of a new Standard on Internal Audit, as detailed in paragraphs 4.1 through 4.8 will be followed.
- 4.10 Subsequent to the issuance of a Standard on Internal Audit, some aspect(s) may require revision which are not

substantive in nature. For this purpose, the Institute of Chartered Accountants of India may make limited revision to a Standard on Internal Audit. The procedure followed for the limited revision will substantially be the same as that to be followed for formulation of a Standard on Internal Audit, ensuring that sufficient opportunity is given to various interest groups and general public to react to the proposal for limited revision.

5. Procedure for Issuing the Guidance Notes on Internal Audit

Broadly, the following procedure will be adopted for issuing Guidance Notes on internal audit.

- 5.1 The Committee will identify the issues on which Guidance Notes need to be formulated and the priority in regard to selection thereof.
- 5.2 In the preparation of the Guidance Notes, the Committee will be assisted by Study Groups constituted to consider specific subjects. In the formation of the Study Groups, provision will be made for participation of a cross section of members of the Institute. In situations considered necessary, the Committee may also consider having an expert on such Study Groups, subject to such terms and conditions, as may be finalised by the Committee. Such expert need not necessarily be a member of the Institute of Chartered Accountants of India. The Study Group will be responsible for preparing the draft of the Guidance Note.
- 5.3 The above mentioned draft Guidance Note would be considered by the Committee. On the basis of the deliberations of the Committee on the draft Guidance Note, the draft of the proposed Guidance Note will be finalised by the Committee and submitted for the consideration of the Council of the Institute. Unlike Standards on Internal Audit, ordinarily, no proposed Guidance Note will be required to be exposed for comments of the members and others. However, in situations considered necessary by the Committee, an Exposure Draft of a Guidance Note may as well be issued for comments. In case an Exposure Draft of

a Guidance Note is issued, the same procedures as required for an Exposure Draft of an SIA (listed in paragraphs 4.3 through 4.8 above) will be required to be followed.

- 5.4 The Council of the Institute will consider the final draft of the proposed Guidance Note and, if necessary, modify the same in consultation with the Committee on Internal Audit. The Guidance Note will then be issued under the authority of the Council.

6. Compliance with the Standards and Guidance Notes on Internal Audit

- 6.1 The SIA(s) will be mandatory from the respective date(s) mentioned in the SIA(s). However, any limitation in the applicability of a specific Standard shall be made clear in the Standard. The mandatory status of a Standard on Internal Audit implies that while carrying out an internal audit, it shall be the duty of the members of the Institute to ensure that the SIAs are followed. If, for any reason, a member has not been able to perform all or any of such activities, as mentioned before, in accordance with the SIAs, his report should draw attention to the material departures therefrom.
- 6.2 Guidance Notes on internal audit are primarily designed to provide guidance to the members on matters which may arise in the course of their internal audit work and on which they may desire assistance in resolving issues which may pose difficulty. The Guidance Notes on internal audit will be recommendatory in nature. A member should, ordinarily, follow recommendations in a Guidance Note on internal audit except where he is satisfied that in the circumstances of the case, it may not be necessary to do so.
- 6.3 If any Standard or Guidance Note on Internal Audit is in variance/conflicts with any circular/notification/any such direction issued by any regulatory authority, the latter shall prevail. The member should, however, describe this fact in their internal audit report.

Training Material on Internal Audit

- 6.4 Whenever any specific Standard on Internal Audit is issued by the ICAI for which any Guidance Note is already in existence, then the date on which the Standard comes into effect, the Guidance Note shall stand withdrawn. Guidance Note will be ceased to exist from the date when Standard on Internal Audit is made applicable.

7. Effective Date

- 7.1 Members will be expected to follow SIAs in the internal audits commencing on or after the date(s) specified in the Standard.

APPENDIX II

FRAMEWORK FOR STANDARDS ON INTERNAL AUDIT*

CONTENTS

	Paragraph(s)
Introduction and scope	1-5
Components of the Framework.....	6-11
<i>The Code of Conduct</i>	7-8
<i>The Competence Framework</i>	9
<i>The Body of Standards</i>	10
<i>The Technical Guidance</i>	11
Authority	12

* Published in the October 2008 issue of *The Chartered Accountant*.

Introduction and Scope

1. In February 2004, the Institute of Chartered Accountants of India, set-up the Committee on Internal Audit. The main function of the Committee on Internal Audit, as set out in its Terms of Reference and the Preface to the Standards on Internal Audit, is to review the existing internal audit practices in India and to develop Standards on Internal Audit (SIAs).
2. Paragraph 3.1 of the Preface to the Standards on Internal Audit, issued by the Council of the Institute of Chartered Accountants of India in 2004, describes internal audit as follows:

“Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system.”
3. Every standard setting process requires a framework, hence the need for this Framework for Standards on Internal Audit. The overall objective of the Framework for Standards on Internal Audit is to promote professionalism in the internal audit activity.
4. Internal audit is conducted in variant economic, legal, cultural and business environments. The organisations in which internal audit is performed differ widely in size, structure, nature of business, scale, purpose, objectives and geographical spread. Further, the internal audit activity may be performed by an entity’s employees or by some external agency. Thus, the Framework for Standards on Internal Audit applies to all the persons performing internal audit activity, irrespective of whether the function is performed in-house or by an external agency.
5. The Framework for Standards on Internal Audit would cover all aspects of an internal audit activity, including, planning,

gathering evidence, documentation, using the work of other experts, evaluating controls and risk management systems and reporting.

Components of the Framework

6. The Framework for Standards on Internal Audit comprises four components viz, the Code of Conduct, the Competence Framework, the Body of Standards and the Technical Guidance. Each of these components has been discussed in the following paragraphs.

The Code of Conduct

7. The Code of Conduct establishes the essential principles of conduct and prescribes ethical behaviour for the professionals in internal audit activity. Every professional must make a commitment to ethical conduct, including integrity, confidentiality, etc.
8. A member of the Institute of Chartered Accountants of India, carrying out an internal audit activity, would additionally be governed by:
 - (i) the requirements of the Chartered Accountants Act, 1949;
 - (ii) the Code of Ethics issued by the Institute of Chartered Accountants of India; and
 - (iii) other relevant pronouncements of the Institute of Chartered Accountants of India.

The Competence Framework

9. The Competence Framework addresses the key characteristics that are required of persons performing internal audit. This includes aspects, such as, objectivity, technical competence, interpersonal skills, operational efficiency and due professional care. The Competence Framework is a minimum expectation.

The Body of Standards

10. The Body of Standards ensures commitment to providing quality services and details the expectations required of the individuals engaged in internal audit in discharging their responsibilities. The Standards will specify basic principles and processes, such as defining the scope, planning, communicating, etc. They will further establish the basis for quality and performance evaluation of internal audit. The Body of Standards are mandatory minimum requirements that all the internal auditors must meet.

The Technical Guidance

11. Technical Guidance can take two forms. It will include explanatory material on the Standards or it may detail the application of Standards in specific industries or situations in the form of Technical Guides. These Technical Guides would, therefore, provide guidance to internal auditors in resolving professional issues arising during the course of an internal audit while discharging their duties as internal auditors.

Authority

12. The first three components of the Framework for Standards on Internal Audit viz., the Code of Conduct, the Competence Framework and the Body of Standards shall be mandatory. Compliance with the mandatory elements of the Framework for Standards on Internal Audit is necessary to meet the responsibilities placed upon the internal auditors in execution of their work since the internal audit activity is carried out at the behest of the governing body and/or the management of an entity and renders service by assessing and reporting upon the effectiveness of issues related to governance, risk and controls and making recommendations for improvements in these areas.

APPENDIX III

STANDARD ON INTERNAL AUDIT (SIA) 1 PLANNING AN INTERNAL AUDIT*

CONTENTS

	Paragraph(s)
Objectives of Planning	1-6
Factor affecting the Planning Process	7
Scope of planning	8-9
Planning process	10-19
Effective Date	20

The following is the text of the Standard on Internal Audit (SIA) 1, "Planning an Internal Audit", issued by the Council of the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the Preface to the Standards on Internal Audit, issued by the Institute.

In terms of the decision of the Council of the Institute of Chartered Accountants of India taken at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as notified by the Council.

* Published in the September 2006 issue of *The Chartered Accountant*.

Objectives of Planning

1. The purpose of this Standard on Internal Audit is to establish standards and provide guidance in respect of planning an internal audit. An internal audit plan is a document defining the scope, coverage and resources, including time, required for an internal audit over a defined period. **The internal auditor should, in consultation with those charged with governance, including the audit committee, develop and document a plan for each internal audit engagement to help him conduct the engagement in an efficient and timely manner.** Adequate planning ensures that appropriate attention is devoted to significant areas of audit, potential problems are identified, and that the skills and time of the staff are appropriately utilised. Planning also ensures that the work is carried out in accordance with the applicable pronouncements of the Institute of Chartered Accountants of India.

2. The overall objectives of an internal audit, as defined in the Preface to the Standards and Guidance Notes on Internal Audit are:

- to suggest improvements to the functioning of the entity; and
 - to strengthen the overall governance mechanism of the entity, including its strategic risk management as well as internal control system.
3. Internal audit, therefore, helps *inter alia* in:
- (i) Understanding and assessing the risks and evaluate the adequacies of the prevalent internal controls.
 - (ii) Identifying areas for systems improvement and strengthening controls.
 - (iii) Ensuring optimum utilisation of the resources of the entity, for example, human resources, physical resources etc.
 - (iv) Ensuring proper and timely identification of liabilities, including contingent liabilities of the entity.

- (v) Ensuring compliance with internal and external guidelines and policies of the entity as well as the applicable statutory and regulatory requirements.
- (vi) Safeguarding the assets of the entity.
- (vii) Reviewing and ensuring adequacy of information systems security and control.
- (viii) Reviewing and ensuring adequacy, relevance, reliability and timeliness of management information system.

4. The internal audit plan should be comprehensive enough to ensure that it helps in achieving of the above overall objectives of an internal audit. The internal audit plan should, generally, also be consistent with the goals and objectives of the internal audit function as listed out in the internal audit charter as well as the goals and objectives of the organisation. An internal audit charter is an important document defining the position of the internal audit *vis a vis* the organisation. The internal audit charter also outlines the scope of internal audit as well as the duties, responsibilities and powers of the internal auditor(s). In case the entire internal audit or the particular internal audit engagement has been outsourced, the internal auditor should also ensure that the plan is consistent with the terms of the engagement.

5. Planning involves developing an overall plan for the expected scope and conduct of audit and developing an audit programme showing the nature, timing and extent of audit procedures. Planning is a continuous exercise. A plan once prepared should be continuously reviewed by the internal auditor to identify any modifications required to bring the same in line with the changes, if any, in the audit environment. However, any major modification to the internal audit plan should be done in consultation with those charged with governance. Further, the internal auditor should also document the changes to the internal audit plan.

6. The internal auditor may also discuss the significant elements of his overall plan, including important procedures, with those charged with governance. This would help the internal auditor as well as the client to assess whether the internal audit is directed to achieve the objectives as set out in the terms of engagement. The discussion would also help the internal auditor to gauge whether the client's perception of the role and responsibilities of the internal auditor is appropriate. The internal auditor should also assess the client expectations as to the assurance level on different aspect of entity's operations and controls. For instance, the client may feel assured if inventories are verified once in a quarter, while for cash verification, monthly interval may be specified. This will enable the auditor to plan the frequency and extent of audit procedures to be adopted.

Factors Affecting the Planning Process

7. The internal audit plan should be based on the knowledge of the entity's business. While developing the internal audit plan, the internal auditor should have regard to the objectives of the internal audit engagement as well as the time and resources required for conducting the engagement. In addition, the internal audit plan should also reflect the risk management strategy of the entity. Planning an internal audit involves establishing the overall strategy for the engagement so as to keep the risks associated with the assignment at the acceptable level. Therefore, the planning process is also influenced by the internal auditor's understanding and assessment of:

- The objectives of the activity being subjected to internal audit.
- The significant risks associated with the above activity.
- The risk management and internal control system instituted in the organisation to reduce the above risks to an acceptable level.
- The possible areas in which the internal audit can suggest improvement to the risk management and/ or internal control system associated with the concerned activity.

- The selection of engagement team (including, where necessary, the engagement team quality control reviewer) and the assignment of audit work to the team members, including the assignment of appropriately experienced team members.
- Business developments affecting the entity, including changes in information technology and business processes, changes in key management, and acquisitions, mergers and divestments.
- Industry developments such as changes in industry regulations and new reporting requirements.
- Changes in the financial reporting framework, such as changes in accounting standards.
- Other significant relevant developments, such as changes in the legal environment affecting the entity.

Scope of Planning

8. Internal audit plan should cover areas such as:

- **Obtaining the knowledge of the legal and regulatory framework within which the entity operates.**
- **Obtaining the knowledge of the entity's accounting and internal control systems and policies.**
- **Determining the effectiveness of the internal control procedures adopted by the entity.**
- **Determining the nature, timing and extent of procedures to be performed.**
- **Identifying the activities warranting special focus based on the materiality and criticality of such activities, and their overall effect on operations of the entity.**

- **Identifying and allocating staff to the different activities to be undertaken.**
- **Setting the time budget for each of the activities.**
- **Identifying the reporting responsibilities.**

The internal audit plan should also identify the benchmarks against which the actual results of the activities, the actual time spent, the cost incurred would be measured.

9. The scope of an internal audit is normally affected by factors such as:

- Terms of the engagement.
- Nature of accounting system – manual or IT-based - and the degree of reliance placed by the auditor on the same.
- Accounting policies adopted by the entity.
- Nature of information technology system used by the client in the various business processes and the exception reports generated by the system.
- Authorization and delegation of authority in the systems environment and data entry checks and data security measures including generation of day end logs of security and authorisation violations.
- The nature of management information system in vogue and the extent to which the management information system reports are used by the client in establishing and reviewing internal controls.
- Expected audit coverage, including identification of areas of audit requiring special attention, number and locations to be included, nature of business segments to be audited and the need, if any, for specialized knowledge.
- Materiality thresholds established in respect of various areas of audit especially, those areas requiring special attention.

- Nature and extent of audit evidence to be obtained.
- Experience and skills of the staff and the need for supervising, directing, coordinating and reviewing their work.
- Requirements of the applicable pronouncements of the Institute of Chartered Accountants of India.
- Statutory or regulatory framework in which the entity operates.

Planning Process

Obtaining Knowledge of the Business

10. The internal auditor should obtain a level of knowledge of the entity sufficient to enable him to identify events, transactions, policies and practices that may have a significant effect on the financial information. Following are some of the sources wherefrom the internal auditor can obtain such knowledge :

- Previous experience, if any, with the entity and the industry.
- Legislation and regulations that significantly affect the entity.
- Entity's policy and procedures manual.
- Minutes of the meetings of the shareholders, board of directors, and important committees of the board such as the audit committee, remuneration committee, shareholders' grievances committee.
- Management reports/ internal audit reports of prior periods.
- Newspaper/ industry journals.
- Discussion with client's management and staff.
- Visits to entity's plant facilities etc., to obtain first hand information regarding the production processes of the entity.

Training Material on Internal Audit

- Visits to the entity's department where the accounting and other documents are generated, maintained, and the administrative procedures followed.
- Other documents produced by the entity, for example, material sent to the shareholders and the regulatory authorities, management policy manuals, manuals relating to accounting and internal controls, organizational charts, job description charts, etc.

Knowledge of the entity's business, among other things, helps the internal auditor to identify areas requiring special focus, evaluate the appropriateness of the accounting policies and disclosures, accounting estimates and management representations. Knowledge of the business would also help the auditor to identify the priorities of the business, critical factors or constraints in the smooth running of the business as also understand the trends in respect of various financial and operating ratios, etc.

Establishing the Audit Universe

11. The next step in audit planning is establishment of the audit universe or the audit territory. Audit universe comprises the activities, operations, units etc., to be subjected to audit during the planning period. The audit universe is designed to reflect the overall business objectives and therefore includes components from the strategic plan of the entity. Thus, the audit universe is affected by the risk management process of the client. **The audit universe and the related audit plan should also reflect changes in the management's course of action, corporate objectives, etc.**

12. As discussed in paragraph 4, planning is a continuous exercise. **The internal auditor should periodically, say half yearly, review the audit universe to identify any changes therein and make necessary amendments, to make the audit plan responsive to those changes.**

Establishing the Objectives of the Engagement

13. The next stage in planning is establishing the specific objectives of the internal audit engagement. **The establishment of such objectives should be based on the auditor's knowledge of the client's business, especially a preliminary understanding and review of the risks and controls associated with the activities forming subject matter of the internal audit engagement.** The preliminary understanding and review involves gathering necessary information by means of a combination of the following procedures:

- Observation of the activity being performed.
- Inquiry of the staff associated with performing the activity.
- Discussion with the client.
- Reading through the internal audit reports, management reports etc., of previous periods.
- Performing analytical procedures.
- Performing actual walk-through tests.

14. The internal auditor would use the information so gathered to determine the objective(s) of the engagement as also to decide the nature, timing and extent of his procedures. **The internal auditor should also document the results of his preliminary review so conducted.** The documented results would, normally, cover aspects such as:

- Preliminary assessment and understanding the risks and controls associated with the activity, viz., sufficiency and appropriateness of the controls, procedures for identification and management of risks associated with the activity.
- Significant issues thrown up by such a review, for example, significant errors, non-compliance with any significant law.

Training Material on Internal Audit

- Procedures proposed to be adopted by the internal auditor to resolve the above issues.
- Preliminary time budget for completing the engagement.

Establishing the Scope of the Engagement

15. The next stage in planning an internal audit is establishing the scope of the engagement. The scope of the engagement should be sufficient in coverage so as to meet the objectives of the engagement. The internal auditor should consider the information gathered during the preliminary review stage to determine the scope of his audit procedures. The nature and extent of the internal auditor's procedures would also be affected by the terms of the engagement. In case the internal auditor is of the view that circumstances exist which would restrict the auditor from carrying out the procedures, including any alternative procedures, considered necessary by him, he should discuss the matter with the client to reach a conclusion whether or not to continue the engagement. The scope of his engagement should be documented comprehensively to avoid misunderstanding on the areas covered for audit. The internal auditors are often confronted with a situation where client denies access to certain information or has a negative list of areas where internal audit is not desired. There are also situations where while the client requires internal audit procedures to be carried but findings are not to form part of the report but to be reported separately.

16. Further, in case of information technology based environment, the scope of engagement would include the extent to which internal auditor are permitted to access the system and reports which can be viewed and those which can be exported. Further, system based audit tools that an internal auditor can use to draw and analyze the data should be clearly understood in the scope of his engagement.

Deciding the Resource Allocation

17. Once the scope of the internal audit procedures is established, the next phase is that of deciding upon the resource allocation. Efficient resource allocation is essential to achieve the desired objective, within the constraints of time and cost as well as optimum utilization of resources. **For this purpose, the internal auditor should prepare an audit work schedule, detailing aspects such as:**

- **activities/ procedures to be performed;**
- **engagement team responsible for performing these activities/ procedures; and**
- **time allocated to each of these activities/ procedures.**

18. While preparing the work schedule, the internal auditor should have regard to aspects such as:

- **any significant changes to the entity's missions and objectives, business processes, and management's strategies to counter these changes, for example, changes in the entity's controls structure or changes in the risk assessment and management structures**
- **any changes or proposed changes to the governance structure of the entity**
- **composition of the engagement team in terms of skills and experience and any changes thereto**

The engagement work schedule should, however, be flexible enough to accommodate any unanticipated changes as well as professional judgment of the engagement team in the components of the audit universe as discussed above. The work schedule should also reflect the internal auditor's assessment of risks associated with various areas covered by the particular internal audit engagement and the priority attached thereto.

Preparation of Audit Programme

19 The internal auditor should also prepare a formal internal audit programme listing the procedures essential for meeting the objective of the internal audit plan. Though the form and content of the audit programme and the extent of its details would vary with the circumstances of each case, yet the internal audit programme should be so designed as to achieve the objectives of the engagement and also provide assurance that the internal audit is carried out in accordance with the Standards on Internal Audit. As a corollary, the audit plan developed by the internal auditor would need to be a risk-based plans, appropriately reflecting and addressing the priorities of the internal audit activity, consistent with the organisation's goals. **The internal audit programme should also be finalised in consultation with the appropriate authority before the commencement of the work.** The internal audit programme identifies, in appropriate details, the objectives of the internal audit in respect of each area, the procedures to be performed to achieve those objectives, the staff responsible for carrying out the particular activity, the time allocated to each activity as also the sufficiently detailed, instructions to the staff as to how to carry out those procedures. The internal audit programme may also have provision for information such as the procedures actually performed, reasons for not performing the originally identified procedures, actual time consumed in carrying out the relevant procedure, reasons for deviations from budgeted time etc. A well prepared, comprehensive audit programme helps proper execution of the work as well as of the proper supervision, direction and control of the performance of the engagement team.

Effective Date

20. This Standard on Internal Audit is applicable to all internal audits commencing on or after
Earlier application of the SIA is encouraged.

APPENDIX IV

STANDARD ON INTERNAL AUDIT (SIA) 2 BASIC PRINCIPLES GOVERNING INTERNAL AUDIT*

CONTENTS

	Paragraph(s)
Introduction	1-3
Integrity, Objectivity and Independence	4
Confidentiality	5
Due Professional Care, Skills and Competence	6-8
Work Performed by Others	9
Documentation	10
Planning	11-13
Evidence	14
Internal Control and Risk Management Systems	15
Reporting	16
Effective Date	17

The following is the text of the Standard on Internal Audit (SIA) 2 “*Basic Principles Governing Internal Audit*”, issued by the Council of the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the Preface to the Standards on Internal Audit, issued by the Institute.

In terms of the decision of the Council of the Institute of Chartered Accountants of India taken at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as notified by the Council.

* Published in the August 2007 issue of *The Chartered Accountant*.

Introduction

1. The purpose of this Standard on Internal Audit (SIA) is to establish standards and provide guidance on the general principles governing internal audit.

2. Paragraph 3.1 of the Preface to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India defines internal audit as follows:

“Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s risk management and internal control system.”

3. The other Standards on Internal Audit to be issued by the Institute of Chartered Accountants of India will elaborate the principles set out herein to give guidance on internal auditing procedures and reporting practices. Compliance with the basic principles requires the application of internal auditing procedures and reporting practices appropriate to the particular circumstances.

Integrity, Objectivity and Independence

4. The internal auditor should be straightforward, honest and sincere in his approach to his professional work. He must be fair and must not allow prejudice or bias to override his objectivity. **He should maintain an impartial attitude. He should not only be independent in fact but also appear to be independent. The internal auditor should not, therefore, to the extent possible, undertake activities, which are or might appear to be incompatible with his independence and objectivity.** For example, to avoid any conflict of interest, the internal auditor should not review an activity for which he was previously responsible. It is also expected from the management to take steps necessary for providing an environment conducive to enable the internal auditor to discharge his responsibilities independently and also report his findings without any management interference. For example, in case of a listed company, the internal auditor may be required to report directly to

those charged with governance, such as the Audit Committee instead of the Chief Executive Officer or the Chief Financial Officer. **The internal auditor should immediately bring any actual or apparent conflict of interest to the attention of the appropriate level of management so that necessary corrective action may be taken.**

Confidentiality

5. **The internal auditor should maintain the confidentiality of the information acquired in the course of his work and should not disclose any such information to a third party, including the employees of the entity, without the specific authority of the management/ client or unless there is a legal or a professional responsibility to do so.** The internal auditor, therefore, needs to ensure that there are well laid out policies and controls to protect confidentiality of the information.

Due Professional Care, Skills and Competence

6. **The internal auditor should exercise due professional care, competence and diligence expected of him while carrying out the internal audit.** Due professional care signifies that the internal auditor exercises reasonable care in carrying out the work entrusted to him in terms of deciding on aspects such as the extent of work required to achieve the objectives of the engagement, relative complexity and materiality of the matters subjected to internal audit, assessment of risk management, control and governance processes and cost benefit analysis. Due professional care, however, neither implies nor guarantees infallibility, nor does it require the internal auditor to travel beyond the scope of his engagement.

7. **The internal auditor should either have or obtain such skills and competence, acquired through general education, technical knowledge obtained through study and formal courses, as are necessary for the purpose of discharging his responsibilities.**

8. The internal auditor also has a continuing responsibility to maintain professional knowledge and skills at a level required to ensure that the client or the employer receives the advantage of competent professional service based on the latest developments

in the profession, the economy, the relevant industry and legislation.

Work Performed by Others

9. The internal auditor would often need to delegate work to assistants. **The internal auditor should carefully direct, supervise and review the work delegated to assistants.** Similarly, the internal auditor may also need to use the work performed by other auditors or experts. Though the internal auditor will be entitled to rely on the work performed by other auditors and experts, he should exercise adequate skill and care in ascertaining their competence and skills and also in evaluating, analysing and using the results of the work performed by the experts. He must also look into the assumptions, if any, made by such other experts and obtain reasonable assurance that the work performed by other auditors and experts is adequate for his purposes. **He should be satisfied that he has no reasons to believe that he should not have relied on the work of the expert.** The reliance placed on the work done by the assistants and/ or other auditors and experts notwithstanding, the internal auditor will continue to be responsible for forming his opinion on the areas/ processes being subject to internal audit or his findings.

Documentation

10. **The internal auditor should document matters, which are important in providing evidence that the audit was carried out in accordance with the Standards on Internal Audit and support his findings or the report submitted by him.** In addition, the working papers also help in planning and performing the internal audit, review and supervise the work and most importantly, provide evidence of the work performed to support his findings or the report(s).

Planning

11. **The internal auditor should plan his work to enable him to conduct an effective internal audit in a timely and efficient manner, ensuring that appropriate attention is devoted to significant areas of audit, identification of potential problems and appropriate utilisation of skills and time of the staff.**

12. The internal audit plan should be based on the knowledge of the business of the entity. The internal audit plan would normally cover aspects such as:

- (i) obtaining the knowledge of the legal and regulatory framework within which the entity operates;
- (ii) obtaining the knowledge of the entity's accounting and internal control systems and policies;
- (iii) determining the effectiveness of the internal control procedures adopted by the entity;
- (iv) identifying the activities warranting special focus based on the materiality and criticality of such activities, and its overall effect on presentation of the financial statements of the entity;
- (v) identifying and allocating staff to each of the above activities;
- (vi) determining the nature, timing and extent of procedures to be performed;
- (vii) setting the time budget for each of the above activities;
- (viii) identifying the reporting responsibilities; and
- (ix) benchmark against which the actual results of the activities, the actual time spent, the cost incurred would be measured.

13. A plan once prepared should be continuously reviewed by the internal auditor to identify any modifications to the plan required to bring the same in line with the changes, if any, to the audit universe. Audit universe comprises the activities, operations, units, etc., to be subjected to audit during the planning period.

Evidence

14. The internal auditor should, based on his professional judgment, obtain sufficient appropriate evidence to enable him to draw reasonable conclusions therefrom on which to base his opinion or findings. Factors affecting the professional judgment include the activity under audit, possible errors and their materiality and the risk of occurrence of such errors.

Internal Control and Risk Management Systems

15. While the management is responsible for establishment and maintenance of appropriate internal control and risk management systems, the role of the internal auditor is to suggest improvements to those systems. **For this purpose, the internal auditor should:**

- (i) **Obtain an understanding of the risk management and internal control framework established and implemented by the management.**
- (ii) **Perform steps for assessing the adequacy of the framework developed in relation to the organisational set up and structure.**
- (iii) **Review the adequacy of the framework.**
- (iv) **Perform risk-based audits on the basis of risk assessment process.**

Internal auditor may, however, also undertake work involving identification of risks as well as recommend design of controls or gaps in existing controls to address those risks.

Reporting

16. **The internal auditor should carefully review and assess the conclusions drawn from the audit evidence obtained, as the basis for his findings contained in his report and suggest remedial action.** However, in case the internal auditor comes across any actual or suspected fraud or any other misappropriation of assets, it would be more appropriate for him to bring the same immediately to the attention of the management.

Effective Date

17. This Standard on Internal Audit is effective for all internal audits beginning on or after..... Earlier application of the SIA is encouraged.

APPENDIX V

STANDARD ON INTERNAL AUDIT (SIA) 3 DOCUMENTATION*

CONTENTS

	Paragraph(s)
Introduction	1-2
Definitions	3-4
Form and Content	5-10
Identification of the Preparer and the Reviewer	11-13
Document Retention and Access.....	14-15
Effective Date.....	16

The following is the text of the Standard on Internal Audit (SIA) 3 “*Documentation*”, issued by the Council of the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the Preface to the Standards on Internal Audit, issued by the Institute.

In terms of the decision of the Council of the Institute of Chartered Accountants of India taken at its 260th meeting held in June, 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as notified by the Council.

* Published in the August 2007 issue of *The Chartered Accountant*.

Introduction

1. The purpose of this Standard on Internal Audit (SIA) is to establish Standards and provide guidance on the documentation requirements in an internal audit.
2. Paragraph 10 of the Standard on Internal Audit (SIA) 2, *Basic Principles Governing Internal Audit*, states as follows:

“10. The internal auditor should document matters, which are important in providing evidence that the audit was carried out in accordance with the Standards on Internal Audit and support his findings or the report submitted by him. In addition, the working papers also help in planning and performing the internal audit, review and supervise the work and most importantly, provide evidence of the work performed to support his findings or report(s).”

Definitions

3. (a) *“Internal audit documentation”* means the record of audit procedures performed, including audit planning as discussed in the Standard on Internal Audit (SIA) 1, *Planning an Internal Audit*, relevant audit evidence obtained, and conclusions the auditor reached (terms such as “working papers” or “workpapers” are also sometimes used). Thus, documentation refers to the working papers prepared or obtained by the internal auditor and retained by him in connection with the performance of his internal audit.
- (b) *“Experienced internal auditor”* or *“a reviewer”* means an individual (whether internal or external to the entity) who has:
 - (i) reasonable knowledge and experience of internal audit processes;

Training Material on Internal Audit

- (ii) reasonable knowledge of SIAs, other relevant pronouncements of the Institute and applicable legal and regulatory requirements;
 - (iii) reasonable understanding of the business environment in which the entity operates; and
 - (iv) reasonable understanding of internal audit issues relevant to the entity's industry.
- 4. Internal audit documentation:
 - Aid in planning and performing the internal audit.
 - Aid in supervision and review of the internal audit work.
 - Provide evidence of the internal audit work performed to support the internal auditor's findings and opinion.
 - Aid in third party reviews, where so done.
 - Provide evidence of the fact that the internal audit was performed in accordance with the scope of work as mentioned in the engagement letter, SIAs and other relevant pronouncements issued by the Institute of Chartered Accountants of India.

Form and Content

5. Internal audit documentation may be recorded on paper or on electronic or other media. It includes, for example, audit programmes, analyses, issues memoranda, summaries of significant matters, letters of confirmation and representation, checklists, and correspondence (including e-mail) concerning significant matters. Abstracts or copies of the entity's records, for example, significant and specific contracts and agreements, may be included as part of internal audit documentation, if considered appropriate. Internal audit documentation, however, is not a substitute for the entity's accounting records. The internal audit documentation for a specific internal audit engagement is assembled in an audit file.

6. Internal audit documentation should record the internal audit charter, the internal audit plan, the nature, timing and extent of audit procedures performed, and the conclusions drawn from the evidence obtained. In case the internal audit is outsourced, the documentation should include a copy of the internal audit engagement letter, containing the terms and conditions of the appointment.

7. Internal audit documentation should be designed and properly organised to meet the requirements and circumstances of each audit and the internal auditor's needs in respect thereof. The internal auditor should formulate policies that help in standardization of the internal audit documentation. The standardization may be in the form of checklists, specimen letters, questionnaires, etc.

8. Internal audit documentation should be sufficiently complete and detailed for an internal auditor to obtain an overall understanding of the audit. The extent of documentation is a matter of professional judgment since it is neither practical nor possible to document every observation, finding or conclusion in the internal audit documentation. **All the significant matters which require exercise of judgment, together with the internal auditor's conclusion thereon should be included in the internal audit documentation. However, the documentation prepared by the internal auditor should be such that enables an experienced internal auditor (or a reviewer), having no previous connection with the internal audit to understand:**

- (a) the nature, timing and extent of the audit procedures performed to comply with SIAs and applicable legal and regulatory requirements;
- (b) the results of the audit procedures and the audit evidence obtained;
- (c) significant matters arising during the audit and the conclusions reached thereon; and
- (d) terms and conditions of an internal audit engagement/requirements of the internal audit charter,

scope of work, reporting requirements, any other special conditions, affecting the internal audit.

9. The form, extent and contents of the documentation would also be affected by the nature and terms of the engagement, and any statutory or regulatory requirements in that regard. The form, content and extent of internal audit documentation depend on factors such as :

- the nature and extent of the audit procedures to be performed;
- the identified risks of material misstatement;
- the extent of judgment required in performing the work and evaluating the results;
- the significance of the audit evidence obtained;
- the nature and extent of exceptions identified;
- the need to document a conclusion or the basis for a conclusion not readily determinable from the documentation of the work performed or audit evidence obtained; and
- the audit methodology and tools used.

It is, however, neither necessary nor practicable to document every matter the auditor considers during the audit.

10. **The internal audit documentation should cover all the important aspects of an engagement viz., engagement acceptance, engagement planning, risk assessment and assessment of internal controls, evidence obtained and examination/ evaluation carried out, review of the findings, communication and reporting and follow up.** The internal audit documentation would, therefore, generally, include:

- Engagement letter or the internal audit charter, as the case may be.
- Internal audit plan and programme.

- Papers relating to the staff requirement and allocation.
- Papers relating to requirements for technical experts, if any .
- Time and cost budgets.
- Copies of significant contracts and agreements or management representations on terms and conditions of those contracts.
- Internal review reports.
- Evaluation questionnaires, checklists, flowcharts, etc.
- Papers relating to discussions/ interviews with the various personnel including legal experts, etc.
- Chart of the organizational structure, job profile of the persons listed in the chart and rules of delegation of powers.
- Annual budget and development plan.
- Progress report, MIS report.
- Reconciliation statements.
- Communication with the client personnel and third parties, if any.
- Certification and representations obtained from management.
- Copies of relevant circulars, extracts of legal provisions.
- Results of risk and internal control assessments.
- Analytical procedures performed and results thereof.
- List of queries and resolution thereof.
- Copy of draft audit report, along with the comments of the auditee thereon and final report issued.

- Records as to the follow up on the recommendations/ findings contained in the report.

Identification of the Preparer and the Reviewer

11. It is also essential that the internal audit documentation identify the following:

- (i) who performed that task and the date such work was completed;
- (ii) who reviewed the task performed and the date and extent of such review;
- (iii) reasons for creating the particular internal audit documentation;
- (iv) source of the information contained in the internal audit documentation; and
- (v) any cross referencing to any other internal audit documentation.

The preparers and reviewers of the internal audit documentation should also sign them.

12. **The internal audit file should be assembled within sixty days after the signing of the internal audit report.** Assembly of the internal audit documentation file is only an administrative process and does not involve performance of any new audit procedures or formulation of new conclusions. Changes may be made to the audit documentation file only if such changes are administrative in nature. For example:

- deleting or discarding superseded documentation;
- sorting, collating and cross referencing internal audit documentation;
- signing off on completion checklists relating to file assembly process;

- documenting audit evidence that the internal auditor has obtained, discussed and agreed with the relevant members of the internal audit team before the date of the internal auditor's report.

13. When exceptional circumstances arise after the date of the submission of the internal audit report that require the internal auditor to perform new or additional audit procedures or that lead the internal auditor to reach new conclusions, the internal auditor should document:

- (i) the details of circumstances encountered along with the documentary evidence, if any, thereof;**
- (ii) the new or additional audit procedures performed, audit evidence obtained, and conclusions reached; and**
- (iii) when and by whom the resulting changes to the audit documentation were made, and (where applicable) reviewed.**

Document Retention and Access

14. The internal auditor should formulate policies as to the custody and retention of the internal audit documentation within the framework of the overall policy of the entity in relation to the retention of documents. The internal auditor retains the ownership of the internal audit documentation. While formulating the documentation retention policy, any legal or regulatory requirements in this regard also need to be taken into consideration. Management and other designated personnel may seek access to the internal audit documentation of the internal audit department subject to the approval of the internal auditor and client or such other third party may seek access if there is any legal or regulatory requirement or as may be permitted by the client.

15. **After the assembly of the audit file, the internal auditor should not delete or discard internal audit documentation before the end of the retention period.**

Effective Date

16. This Standard on Internal Audit will apply to all internal audits commencing on or after Earlier application of the SIA is encouraged.

APPENDIX VI

STANDARD ON INTERNAL AUDIT (SIA) 4 REPORTING

CONTENTS

	Paragraph(s)
Introduction	1-4
Basic Elements of the Internal Audit Report	5-24
Communication to Management	25
Limitation on Scope	26
Restriction on Usage and Report Circulation Otherwise Than to the List of Intended Recipients	27
Effective Date.....	28

The following is the text of the Standard on Internal Audit (SIA) 4, *Reporting*, issued by the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the “*Preface to the Standards on Internal Audit*”, issued by the Institute of Chartered Accountants of India.

In terms of the decision taken by the Council of the Institute at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as notified by the Council.

Introduction

1. The purpose of this Standard on Internal Audit (SIA) is to establish standards on the form and content of the internal auditor's report issued as a result of an internal audit performed by an internal auditor of the systems, processes, controls including items of financial statements of an entity.
2. **The internal auditor should review and assess the analysis drawn from the internal audit evidence obtained as the basis for his conclusion on the efficiency and effectiveness of systems, processes and controls including items of financial statements.**
3. This review and assessment involves considering whether the systems, procedures and controls are in existence and are operating effectively.
4. **The internal auditor's report should contain a clear written expression of significant observations, suggestions/ recommendations based on the policies, processes, risks, controls and transaction processing taken as a whole and managements' responses.**

Basic Elements of the Internal Audit Report

5. The internal auditor's report includes the following basic elements, ordinarily, in the following layout:
 - (a) Title;
 - (b) Addressee;
 - (c) Report Distribution List;
 - (d) Period of coverage of the Report;
 - (e) Opening or introductory paragraph;
 - (i) identification of the processes/functions and items of financial statements audited; and
 - (ii) a statement of the responsibility of the entity's management and the responsibility of the internal auditor;

- (f) Objectives paragraph - statement of the objectives and scope of the internal audit engagement;
- (g) Scope paragraph (describing the nature of an internal audit):
 - (i) a reference to the generally accepted audit procedures in India, as applicable;
 - (ii) a description of the engagement background and the methodology of the internal audit together with procedures performed by the internal auditor; and
 - (iii) a description of the population and the sampling technique used.
- (h) Executive Summary, highlighting the key material issues, observations, control weaknesses and exceptions;
- (i) Observations, findings and recommendations made by the internal auditor;
- (j) Comments from the local management;
- (k) Action Taken Report – Action taken/ not taken pursuant to the observations made in the previous internal audit reports;
- (l) Date of the report;
- (m) Place of signature; and
- (n) Internal auditor's signature with Membership Number.

A measure of uniformity in the form and content of the internal auditor's report is desirable because it helps to promote the reader's understanding of the internal auditor's report and to identify unusual circumstances when they occur.

6. The internal auditor should exercise due professional care to ensure that the internal audit report, inter alia, is:
- (i) clear
 - (ii) factual – presents all significant matters with disclosure of material facts
 - (iii) specific
 - (iv) concise
 - (v) unambiguous
 - (vi) timely
 - (vii) complies with generally accepted audit procedures in India, as applicable.

Title

7. The internal auditor's report should have an appropriate title expressing the nature of the Report.

Addressee

8. The internal auditor's report should be appropriately addressed as required by the circumstances of the engagement. Ordinarily, the internal auditor's report is addressed to the appointing authority or such other person as directed.

Report Distribution List, Coverage and Opening or Introductory Paragraph

9. There should be a mention of the recipients of the report in the section on Report Distribution List.
10. The internal auditor's report should identify the systems, processes, functional lines or other items of the entity that have been audited, including the date of and period covered.

11. **The report should include a statement that the operation of systems, procedures and controls are the responsibility of the entity's management and a statement that the responsibility of the internal auditor is to express an opinion on the weaknesses in internal controls, risk management and governance (entity level controls) framework, highlighting any exceptions and cases of non-compliance and suggest or recommend improvements in the design and operations of controls based on the internal audit.**

Scope Paragraph

12. **The internal auditor's report should describe the scope of the internal audit by stating that the internal audit was conducted in accordance with generally accepted audit procedures as applicable.** The management needs this as an assurance that the audit has been carried out in accordance with established Standards.
13. "Scope" refers to the internal auditor's ability to perform internal audit procedures deemed necessary in the circumstances.
14. **The report should include a statement that the internal audit was planned and performed to obtain reasonable assurance whether the systems, processes and controls operate efficiently and effectively and financial information is free of material misstatement.**
15. **The internal auditor's report, in line with the terms of the engagement, should describe the internal audit as including:**
 - (a) **examining, on a test basis, evidence to support the amounts and disclosures in financial statements;**
 - (b) **assessing the strength, design and operating effectiveness of internal controls at process level and identifying areas of control weakness, business risks and vulnerability in the system and procedures adopted by the entity**

- (c) assessing the accounting principles and estimates used in the preparation of the financial statements; and
 - (d) evaluating the overall entity-wide risk management and governance framework.
16. The Report should include a description of the engagement background, internal audit methodology used and procedures performed by the internal auditor mentioning further that the internal audit provides a reasonable basis for his comments.

Executive Summary Paragraph

17. The Executive Summary paragraph of the internal auditor's report should clearly indicate the highlights of the internal audit findings, key issues and observations of concern, significant controls lapses, failures or weaknesses in the systems or processes.

Observations (Main Report) Paragraph

18. The Observations paragraph should clearly mention the process name, significant observations, findings, analysis and comments of the internal auditor.

Comments from Local Management

19. The Comments from Local Management Paragraph should contain the observations and comments from the local management of the entity provided after giving due cognizance to the internal auditor's comments. This should also include local management's action plan for resolution of the issues and compliance to the internal auditor's recommendations and suggestions on the areas of process and control weakness/ deficiency. The management action plan, should contain, inter alia :
- (a) the timeframe for taking appropriate corrective action;
 - (b) the person responsible; and

- (c) **resource requirements, if any, for ensuring such compliance.**

20. Further comments from the internal auditor, in response to the auditee feedback, are to be clearly mentioned. **This paragraph should also contain the internal auditor's suggestions and recommendations to mitigate risks, strengthen controls and streamline processes with respect to each of the observations and comments made.**

Action Taken Report Paragraph

21. **The Action Taken Report paragraph should be appended after the observations and findings and should include:**
- (a) **Status of compliance / corrective action already taken / being taken by the auditee with respect to previous internal audit observations;**
 - (b) **Status of compliance / corrective action not taken by the auditee with respect to previous internal audit observations and the reasons for non-compliance thereof; and**
 - (c) **Revised timelines for compliance of all open items in (b) above and fixation of the responsibility of the concerned process owner.**

Date

22. The date of an internal auditor's report is the date on which the internal auditor signs the report expressing his comments and observations.

Place of Signature

23. **The report should name the specific location, which is ordinarily the city where the internal audit report is signed.**

Internal Auditor's Signature

24. The report should be signed by the internal auditor in his personal name. The internal auditor should also mention the membership number assigned by the Institute of Chartered Accountants of India in the report so issued by him.

Communication to Management

25. The internal audit report contains the observations and comments of the internal auditor, presents the audit findings, and discusses recommendations for improvements. To facilitate communication and ensure that the recommendations presented in the final report are practical from the point of view of implementation, the internal auditor should discuss the draft with the entity's management prior to issuing the final report. The different stages of communication and discussion should be as under:
 - (a) **Discussion Draft** - At the conclusion of fieldwork, the internal auditor should draft the report after thoroughly reviewing his working papers and the discussion draft before it is presented to the entity's management for auditee's comments. This discussion draft should be submitted to the entity management for their review before the exit meeting.
 - (b) **Exit Meeting** - The internal auditor should discuss with the management of the entity regarding the findings, observations, recommendations, and text of the discussion draft. At this meeting, the entity's management should comment on the draft and the internal audit team should work to achieve consensus and reach an agreement on the internal audit findings.
 - (c) **Formal Draft** - The internal auditor should then prepare a formal draft, taking into account any revision or modification resulting from the exit

meeting and other discussions. When the changes have been reviewed by the internal auditor and the entity management, the final report should be issued.

- (d) *Final Report* - The internal auditor should submit the final report to the appointing authority or such members of management, as directed. The periodicity of the Report should be as agreed in the scope of the internal audit engagement. The internal auditor should mention in the Report, the dates of discussion draft, exit meeting, Formal Draft and Final Report.

Limitation on Scope

- 26. When there is a limitation on the scope of the internal auditor's work, the internal auditor's report should describe the limitation.

Restriction on Usage and Report Circulation Otherwise Than to the List of Intended Recipients

- 27. The internal auditor should state in the Report that the same is to be used for the intended purpose only as agreed upon and the circulation of the Report should be limited to the recipients mentioned in the Report Distribution List.

Effective Date

- 28. This Standard on Internal Audit is applicable to all internal audits commencing on or after _____. Earlier application of the SIA is encouraged.

APPENDIX VII

STANDARD ON INTERNAL AUDIT (SIA) 5 SAMPLING

CONTENTS

	Paragraph(s)
Introduction	1-2
Definitions	3-9
Use of Sampling in Risk Assessment Procedures and Tests of Controls	10-12
Design of the Sample	13-19
Sample Size	20-21
Statistical and Non-Statistical Approaches	22-26
Selection of the Sample	27-28
Evaluation of Sample Results	29-38
Documentation	39
Effective Date	40
<i>Examples of Factors Influencing Sample Size for Tests of Controls</i>	
<i>Examples of Factors Influencing Sample Size for Tests of Details (TOD)</i>	

Methods of Sample Selection

Frequency of Control Activity and Sample Size

The following is the text of the Standard on Internal Audit (SIA) 5, *Sampling*, issued by the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the “*Preface to the Standards on Internal Audit*”, issued by the Institute of Chartered Accountants of India.

In terms of the decision taken by the Council of the Institute at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as notified by the Council.

Introduction

1. The purpose of this Standard on Internal Audit (SIA) is to establish standards on the design and selection of an audit sample and provide guidance on the use of audit sampling in internal audit engagements. The SIA also deals with the evaluation of the sample results. This SIA applies equally to both statistical and non-statistical sampling methods. Either method, when properly applied, can provide sufficient appropriate audit evidence.
2. **When using either statistical or non-statistical sampling methods, the internal auditor should design and select an audit sample, perform audit procedures thereon, and evaluate sample results so as to provide sufficient appropriate audit evidence to meet the objectives of the internal audit engagement unless otherwise specified by the client.**

Definitions

3. "Audit sampling" means the application of audit procedures to less than 100% of the items within an account balance or class of transactions to enable the internal auditor to obtain and evaluate audit evidence about some characteristic of the items selected in order to form a conclusion concerning the population. Certain testing procedures, however, do not come within the definition of sampling. Tests performed on 100% of the items within a population do not involve sampling. Likewise, applying internal audit procedures to all items within a population which have a particular characteristic (for example, all items over a certain amount) does not qualify as audit sampling with respect to the portion of the population examined, nor with regard to the population as a whole, since the items were not selected from the total population on a basis that was expected to be representative. Such items might imply some characteristic of the remaining portion of the population but would not necessarily be the basis for a valid conclusion about the remaining portion of the population.

4. "Error" means either control deviations when performing tests of controls, or misstatements, when performing tests of details.
5. "Population" means the entire set of data from which the sample is selected and about which the internal auditor wishes to draw conclusions. A population may be divided into various strata, or sub-populations, with each stratum being examined separately.
6. "Sampling risk" means the risk that from the possibility that the internal auditor's conclusions, based on examination of a sample may be different from the conclusion reached if the entire population was subjected to the same types of internal audit procedure. The two types of sampling risk are –
 - (a) **The risk that the internal auditor concludes, in the case of tests of controls (TOC), that controls are more effective than they actually are, or in the case of tests of details (TOD), that a material error or misstatement does not exist when in fact it does.**
 - (b) The risk that the internal auditor concludes, in the case of tests of controls (TOC), that controls are less effective than they actually are, or in the case of tests of details (TOD), that a material error or misstatement exists when in fact it does not.

The mathematical complements of these risks are termed confidence levels.
7. "Sampling unit" means the individual items or units constituting a population, for example, credit entries in bank statements, sales invoices or debtors' balances.
8. "Statistical sampling" means any approach to sampling procedure which has the following characteristics –
 - (a) Random selection of a sample; and
 - (b) Use of theory of probability to evaluate sample results, including measurement of sampling risk.
9. "Tolerable error" means the maximum error in a population that the internal auditor is willing to accept.

Use of Sampling in Risk Assessment Procedures and Tests of Controls

10. The internal auditor performs risk assessment procedures to obtain an understanding of the entity, business and its environment, including the mechanism of its internal control. Ordinarily, risk assessment procedures do not involve the use of sampling. However, there are cases, where the internal auditor often plans and performs tests of controls concurrently with obtaining an understanding of the design of controls and examining whether they have been implemented.
11. Tests of controls are performed when the internal auditor's risk assessment includes an expectation of the operating effectiveness of controls. Sampling of tests of controls is appropriate when application of the control leaves audit evidence of performance (for example, initials of the credit manager on a sales invoice indicating formal credit approval).
12. **Sampling risk can be reduced by increasing sample size for both tests of controls and tests of details. Non-sampling risk can be reduced by proper engagement planning, supervision, monitoring and review.**

Design of the Sample

13. **When designing an audit sample, the internal auditor should consider the specific audit objectives, the population from which the internal auditor wishes to sample, and the sample size.**

Internal Audit Objectives

14. The internal auditor would first consider the specific audit objectives to be achieved and the internal audit procedures which are likely to best achieve those objectives. In addition, when internal audit sampling is appropriate, consideration of the nature of the audit evidence sought and possible error conditions or other characteristics relating to that audit evidence will assist the internal auditor in defining what

constitutes an error and what population to use for sampling. For example, when performing tests of controls over an entity's purchasing procedures, the internal auditor will be concerned with matters such as whether an invoice was clerically checked and properly approved. On the other hand, when performing substantive procedures on invoices processed during the period, the internal auditor will be concerned with matters such as the proper reflection of the monetary amounts of such invoices in the periodic financial statements. When performing tests of controls, the internal auditor makes an assessment of the rate of error the internal auditor expects to find in the population to be tested. This assessment is on the basis of the internal auditor's understanding of the design of the relevant controls, and whether they have actually been implemented or the examination of a small number of items from the population.

Population

15. The population is the entire set of data from which the internal auditor wishes to sample in order to reach a conclusion. The internal auditor will need to determine that the population from which the sample is drawn is appropriate for the specific audit objective. For example, if the internal auditor's objective were to test for overstatement of accounts receivable, the population could be defined as the accounts receivable listing. On the other hand, when testing for understatement of accounts payable, the population would not be the accounts payable listing, but rather subsequent disbursements, unpaid invoices, suppliers' statements, unmatched receiving reports, or other populations that would provide audit evidence of understatement of accounts payable.
16. The individual items that make up the population are known as sampling units. The population can be divided into sampling units in a variety of ways. For example, if the internal auditor's objective were to test the validity of accounts receivables, the sampling unit could be defined as customer balances or individual customer invoices. The internal auditor defines the sampling unit in order to obtain

an efficient and effective sample to achieve the particular audit objectives.

17. It is important for the internal auditor to ensure that the population is appropriate to the objective of the internal audit procedure, which will include consideration of the direction of testing. The population also needs to be complete, which means that if the internal auditor intends to use the sample to draw conclusions about whether a control activity operated effectively during the financial reporting period, the population needs to include all relevant items from throughout the entire period.
18. **When performing the audit sampling, the internal auditor performs internal audit procedures to ensure that the information upon which the audit sampling is performed is sufficiently complete and accurate.**

Stratification

19. To assist in the efficient and effective design of the sample, stratification may be appropriate. Stratification is the process of dividing a population into sub-populations, each of which is a group of sampling units, which have similar characteristics (often monetary value). The strata need to be explicitly defined so that each sampling unit can belong to only one stratum. This process reduces the variability of the items within each stratum. Stratification, therefore, enables the internal auditor to direct audit efforts towards the items which, for example, contain the greatest potential monetary error. For example, the internal auditor may direct attention to larger value items for accounts receivable to detect overstated material misstatements. In addition, stratification may result in a smaller sample size.

Sample Size

20. **When determining the sample size, the internal auditor should consider sampling risk, the tolerable error, and the expected error.** The lower the risk that the internal auditor is willing to accept, the greater the sample size needs to be. Examples of some factors affecting sample

size are contained in Appendix 1 and Appendix 2 to the Standard.

21. The sample size can be determined by the application of a statistically based formula or through exercise of professional judgment applied objectively to the circumstances of the particular internal audit engagement.

Statistical and Non-Statistical Approaches

22. The decision of using either statistical or non-statistical sampling approach is a matter for the internal auditor's professional judgment. In the case of tests of controls, the internal auditor's analysis of the nature and cause of errors will often be of more importance than the statistical analysis of the mere presence or absence of errors. In such case, non-statistical sampling approach may be preferred.
23. When applying statistical sampling, sample size may be ascertained using either probability theory or professional judgment. Sample size is a function of several factors. Appendices 1 and 2 discuss some of these factors.

Tolerable Error

24. Tolerable error is the maximum error in the population that the internal auditor would be willing to accept and still conclude that the result from the sample has achieved the objective(s) of the internal audit. Tolerable error is considered during the planning stage and, for substantive procedures, is related to the internal auditor's judgement about materiality. The smaller the tolerable error, the greater the sample size will need to be.
25. In tests of controls, the tolerable error is the maximum rate of deviation from a prescribed control procedure that the internal auditor would be willing to accept, based on the preliminary assessment of control risk. In substantive procedures, the tolerable error is the maximum monetary error in an account balance or class of transactions that the internal auditor would be willing to accept so that when the results of all audit procedures are considered, the internal

auditor is able to conclude, with reasonable assurance, that the financial statements are not materially misstated.

Expected Error

26. If the internal auditor expects error to be present in the population, a larger sample than when no error is expected ordinarily needs to be examined to conclude that the actual error in the population is not greater than the planned tolerable error. Smaller sample sizes are justified when the population is expected to be error free. In determining the expected error in a population, the internal auditor would consider such matters as error levels identified in previous internal audits, changes in the entity's procedures, and evidence available from other procedures.

Selection of the Sample

27. **The internal auditor should select sample items in such a way that the sample can be expected to be representative of the population. This requires that all items or sampling units in the population have an opportunity of being selected.**
28. While there are a number of selection methods, three methods commonly used are:
- Random selection and use of CAATs
 - Systematic selection
 - Haphazard selection

Appendix 3 to the Standard discusses these methods.

Evaluation of Sample Results

29. **Having carried out, on each sample item, those audit procedures that are appropriate to the particular audit objective, the internal auditor should:**
- (a) **analyse the nature and cause of any errors detected in the sample;**

- (b) project the errors found in the sample to the population;
 - (c) reassess the sampling risk; and
 - (d) consider their possible effect on the particular internal audit objective and on other areas of the internal audit engagement.
30. The internal auditor should evaluate the sample results to determine whether the assessment of the relevant characteristics of the population is confirmed or whether it needs to be revised.

Analysis of Errors in the Sample

31. In analysing the errors detected in the sample, the internal auditor will first need to determine that an item in question is in fact an error. In designing the sample, the internal auditor will have defined those conditions that constitute an error by reference to the audit objectives. For example, in a substantive procedure relating to the recording of accounts receivable, a mis-posting between customer accounts does not affect the total accounts receivable. Therefore, it may be inappropriate to consider this an error in evaluating the sample results of this particular procedure, even though it may have an effect on other areas of the audit such as the assessment of doubtful accounts.
32. When the expected audit evidence regarding a specific sample item cannot be obtained, the internal auditor may be able to obtain sufficient appropriate audit evidence through performing alternative procedures. For example, if a positive account receivable confirmation has been requested and no reply was received, the internal auditor may be able to obtain sufficient appropriate audit evidence that the receivable is valid by reviewing subsequent payments from the customer. If the internal auditor does not, or is unable to, perform satisfactory alternative procedures, or if the procedures performed do not enable the internal auditor to obtain sufficient appropriate audit evidence, the item would be treated as an error.

Training Material on Internal Audit

33. The internal auditor would also consider the qualitative aspects of the errors. These include the nature and cause of the error and the possible effect of the error on other phases of the audit.
34. In analysing the errors discovered, the internal auditor may observe that many have a common feature, for example, type of transaction, location, product line, or period of time. In such circumstances, the internal auditor may decide to identify all items in the population which possess the common feature, thereby producing a sub-population, and extend audit procedures in this area. The internal auditor would then perform a separate analysis based on the items examined for each sub-population.

Projection of Errors

35. The internal auditor projects the error results of the sample to the population from which the sample was selected. There are several acceptable methods of projecting error results. However, in all the cases, the method of projection will need to be consistent with the method used to select the sampling unit. When projecting error results, the internal auditor needs to keep in mind the qualitative aspects of the errors found. When the population has been divided into sub-population, the projection of errors is done separately for each sub-population and the results are combined.
36. For tests of controls, no explicit projection of errors is necessary since the sample error rate is also the projected rate of error for the population as a whole.

Reassessing Sampling Risk

37. The internal auditor needs to consider whether errors in the population might exceed the tolerable error. To accomplish this, the internal auditor compares the projected population error to the tolerable error taking into account the results of other audit procedures relevant to the specific control or financial statement assertion. The projected population error used for this comparison in the case of substantive procedures is net of adjustments made by the entity. When

the projected error exceeds tolerable error, the internal auditor reassesses the sampling risk and if that risk is unacceptable, would consider extending the audit procedure or performing alternative internal audit procedures.

38. If the evaluation of sample results indicate that the assessment of the relevant characteristic of the population needs to be revised, the internal auditor, may:
- (a) **Request management to investigate the identified errors and the potential for any further errors, and to make necessary adjustments, in cases where management prescribes the sample size; and / or**
 - (b) Modify the nature, timing and extent of internal audit procedures. In case of tests of controls, the internal auditor might extend the sample size, test an alternative control or modify related substantive procedures; and / or
 - (c) Consider the effect on the Internal Audit Report.

Documentation

39. Documentation provides the essential support to the opinion and/ or findings of the internal auditor. In the context of sampling, the internal auditor's documentation may include aspects such as:
- i. Relationship between the design of the sample *vis a vis* specific audit objectives, population from which sample is drawn and the sample size.
 - ii. Assessment of the expected rate of error in the population to be tested *vis a vis* auditor's understanding of the design of the relevant controls
 - iii. Assessment of the sampling risk and the tolerable error.
 - iv. Assessment of the nature and cause of errors.

Training Material on Internal Audit

- v. Rationale for using a particular sampling technique and results thereof.
- vi. Analysis of the nature and cause of any errors detected in the sample.
- vii. Projection of the errors found in the sample to the population.
- viii. Reassessment of sampling risk, where appropriate.
- ix. Effect of the sample results on the internal audit's objective(s).
- x. Projection of sample results to the characteristics of the population.

Effective Date

40. This Standard on Internal Audit is applicable to all internal audits commencing on or after _____. Earlier application of the SIA is encouraged.

Appendix 1

Examples of Factors Influencing Sample Size for Tests of Controls

The following are some factors which the internal auditor considers when determining the sample size required for tests of controls (TOC). These factors need to be considered together assuming the internal auditor does not modify the nature or timing of TOC or otherwise modify the approach to substantive procedures in response to assessed risks.

<i>Factor to be considered by Internal Auditor</i>	<i>Effect on sample size</i>
An increase in the extent to which the risk of material misstatement is reduced by the operating effectiveness of controls	Increase
An increase in the rate of deviation from the prescribed control activity that the internal auditor is willing to accept	Decrease
An increase in the rate of deviation from the prescribed control activity that the internal auditor expects to find in the population	Increase
An increase in the internal auditor's required confidence level	Increase
An increase in the number of sampling units in the population	Negligible effect

Notes –

1. Other things being equal, the more the internal auditor relies on the operating effectiveness of controls in risk assessment, the greater is the extent of the internal auditor's tests of controls, and hence the sample size is increased.

Training Material on Internal Audit

2. The lower the rate of deviation that the internal auditor is willing to accept, the larger the sample size needs to be.
3. The higher the rate of deviation that the internal auditor expects, the larger the sample size needs to be so as to make a reasonable estimate of the actual rate of deviation.
4. The higher the degree of confidence that the internal auditor requires that the results of the sample are indicative of the actual incidence of errors in the population, the larger the sample size needs to be.
5. For large populations, the actual population size has little effect on sample size. For small populations, sampling is often not as efficient as alternative means of obtaining sufficient appropriate audit evidence.

Appendix 2

Examples of Factors Influencing Sample Size for Tests of Details (TOD)

The following are some factors which the internal auditor considers when determining the sample size required for tests of details (TOD). These factors need to be considered together assuming the internal auditor does not modify the nature or timing of TOD or otherwise modify the approach to substantive procedures in response to assessed risks.

<i>Factor to be considered by Internal Auditor</i>	<i>Effect on sample size</i>
An increase in the internal auditor's assessment of the risk of material misstatement	Increase
An increase in the use of other substantive procedures by the internal auditor, directed at the same assertion	Decrease
An increase in the total error that the internal auditor is willing to accept (Tolerable Error)	Decrease
Stratification of the population when appropriate	Decrease
An increase in the amount of error which the internal auditor expects to find in the population	Increase
An increase in the internal auditor's required confidence level	Increase
The number of sampling units in the population	Negligible effect

Appendix 3

Methods of Sample Selection

The principal methods of sample selection are as –

1. **Using a computerised random number generator** or through random number tables.
2. **Systematic selection** – In this method, the number of sampling units in the population is divided by the sample size to give a sampling interval, for example 20, and having thus determined a starting point within the first 20, each 20th sampling unit thereafter is selected. Although the starting point may be haphazardly determined, the sample is likely to be truly random if the same is determined by using a computerised random number generator or random number tables. In this method, the internal auditor would need to determine that sampling units within the population are not structured in such a way that the sampling interval corresponds with any particular pattern within the population.
3. **Haphazard selection** – In this method, the internal auditor selects the sample without following any structured technique. **The internal auditor should attempt to ensure that all items within the population have a chance of selection, without having any conscious bias or predictability.** This method is not appropriate when using statistical sampling technique.
4. **Block selection** – This method involves selection of a block(s) of adjacent or contiguous items from within the population. Block selection normally cannot be used in internal audit sampling because most populations are structured in such a manner that items forming a sequence can be expected to have similar characteristics to each other, but different characteristics from items elsewhere in the population. This method would not be an appropriate sample selection technique when the internal auditor intends to draw valid inferences about the entire population, based on the sample.

Appendix 4

Frequency of Control Activity and Sample Size

The following guidance related to the frequency of the performance of control may be considered when planning the extent of tests of operating effectiveness of manual controls for which control deviations are not expected to be found. The internal auditor may determine the appropriate number of control occurrences to test based on the following minimum sample size for the frequency of the control activity dependant on whether assessment has been made on a lower or higher risk of failure of the control.

Frequency of control activity	Minimum sample size	
	Risk of failure	
	Lower	Higher
Annual	1	1
Quarterly (including period- end, i.e., +1)	1+1	1+1
Monthly	2	3
Weekly	5	8
Daily	15	25
Recurring manual control (multiple times per day)	25	40

Note

Although +1 is used to indicate that the period–end control is tested, this does not mean that for more frequent control operations the year-end operation cannot be tested.

APPENDIX VIII

STANDARD ON INTERNAL AUDIT (SIA) 6 ANALYTICAL PROCEDURES

CONTENTS

	Paragraph(s)
Introduction	1-3
Nature and Purpose of Analytical Procedures	4-9
Analytical Procedures as Risk Assessment Procedures and in Planning the Internal Audit	10-11
Analytical Procedures as Substantive Procedures	12-14
Analytical Procedures in the Overall Review at the End of the Internal Audit	15
Extent of Reliance on Analytical Procedures	16-18
Investigating Unusual Items or Trends	19-20
Effective Date.....	21

The following is the text of the Standard on Internal Audit (SIA) 6, *Analytical Procedures*, issued by the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the “*Preface to the Standards on Internal Audit*”, issued by the Institute of Chartered Accountants of India.

In terms of the decision taken by the Council of the Institute at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as notified by the Council.

Introduction

1. The purpose of this Standard on Internal Audit (SIA) is to establish standards on the application of analytical procedures during an internal audit.
2. **The internal auditor should apply analytical procedures as the risk assessment procedures at the planning and overall review stages of the internal audit.** Risk assessment procedures refer to the internal audit procedures performed to obtain an understanding of the entity and its environment, including the entity's internal control, to identify and assess the risks of material misstatement, whether due to fraud or error, in the information subjected to internal audit. Analytical procedures may also be applied at other stages.
3. "Analytical procedures" means the analysis of significant ratios and trends, including the resulting investigation of fluctuations and relationships in both financial and non-financial data that are inconsistent with other relevant information or which deviate significantly from predicted amounts. Analytical procedures provide the internal auditor with an efficient and effective means of making an assessment of information collected in an audit. The assessment results from comparing such information with expectations identified or developed by the internal auditor.

Nature and Purpose of Analytical Procedures

4. Analytical procedures include the consideration of comparisons of the entity's financial and non-financial information with, for example:
 - Comparable information for prior periods.
 - Anticipated results of the entity, such as budgets or forecasts or expectations of the internal auditor.

Training Material on Internal Audit

- Predictive estimates prepared by the internal auditor, such as an estimation of depreciation charge for the year.
 - Similar industry information, such as a comparison of the entity's ratio of sales to trade debtors with industry averages, or with other entities of comparable size in the same industry.
5. Analytical procedures also include consideration of relationships:
- Among elements of financial information that would be expected to conform to a predictable pattern based on the entity's experience, such as gross margin percentages.
 - Between financial information and relevant non-financial information, such as payroll costs to number of employees or total production costs to quantity produced.
6. Various methods may be used in performing the above procedures. These range from simple comparisons to complex analyses using advanced statistical techniques. Analytical procedures may be applied to consolidated financial statements, financial statements of components (such as subsidiaries, divisions or segments) and individual elements of financial information and relevant non-financial information. The internal auditor's choice of procedures, methods and level of application is a matter of professional judgement. Specific analytical procedures include, but are not limited to ratio, trend, and regression analysis, reasonableness tests, period-to-period comparisons, comparisons with budgets, forecasts, and external economic information.
7. **In determining the extent to which the analytical procedures should be used, the internal auditor should consider the following factors, including:**
- **The significance of the area being examined.**

- **The adequacy of the system of internal control.**
- **The availability and reliability of financial and non-financial information.**
- **The precision with which the results of analytical procedures can be predicted.**
- **The availability and comparability of information regarding the industry in which the organization operates.**
- **The extent to which other auditing procedures provide support for audit results.**

After evaluating the aforementioned factors, the internal auditor should consider and use additional auditing procedures, as necessary, to achieve the audit objective.

8. Analytical procedures are used for the following purposes:
 - to assist the internal auditor as risk assessment procedures to obtain initial understanding of the entity and its environment and thereafter in planning the nature, timing and extent of other internal audit procedures;
 - as substantive procedures when their use can be more effective or efficient than tests of details in reducing detection risk for specific financial statement assertions;
 - as an overall review of the systems and processes in the final review stage of the internal audit; and
 - to evaluate the efficiency of various business/management systems.
9. Analytical procedures may identify, among other things, differences that are not expected or absence of differences when they are expected, which may have arisen on account of factors such as errors, frauds, unusual or non recurring transaction or events, etc.

Analytical Procedures as Risk Assessment Procedures and in Planning the Internal Audit

10. **The internal auditor should apply analytical procedures as risk assessment procedures to obtain an understanding of the business, the entity and its environment and in identifying areas of potential risk.** Application of analytical procedures may indicate aspects of the business of which the internal auditor was unaware and will assist in determining the nature, timing and extent of other internal audit procedures.
11. Analytical procedures in planning the internal audit use both financial and non-financial information, for example, in retail business, the relationship between sales and square footage of selling space or volume of goods sold.

Analytical Procedures as Substantive Procedures

12. The internal auditor's reliance on substantive procedures to reduce detection risk relating to specific financial statement assertions and assertions relating to process, systems and controls may be derived from tests of details, from analytical procedures, or from a combination of both. The decision about which procedures to use to achieve a particular internal audit objective is based on the internal auditor's judgement about the expected effectiveness and efficiency of the available procedures in reducing detection risk for specific financial statement assertions or assertions relating to process, systems and controls.
13. The internal auditor will ordinarily inquire of management as to the availability and reliability of information needed to apply analytical procedures and the results of any such procedures performed by the entity. It may be efficient to use analytical data prepared by the entity, provided the internal auditor is satisfied that such data is properly prepared.

14. When intending to perform analytical procedures as substantive procedures, the internal auditor will need to consider a number of factors such as the:
- Objectives of the analytical procedures and the extent to which their results can be relied upon.
 - Nature of the business, entity and the degree to which information can be disaggregated.
 - Availability of information, both financial, such as budgets or forecasts, and non-financial, such as the number of units produced or sold.
 - Reliability of the information available, for example, whether budgets is prepared with sufficient professional care.
 - Relevance of the information available, for example, whether budgets have been established as results to be expected rather than as goals to be achieved.
 - Source of the information available, for example, sources independent of the entity are ordinarily more reliable than internal sources.
 - Comparability of the information available, for example, broad industry data may need to be supplemented to be comparable to that of an entity that produces and sells specialised products.
 - Knowledge gained during previous internal audits, together with the internal auditor's understanding of the effectiveness of the accounting and internal control systems and the types of problems that in prior periods have given rise to accounting adjustments.
 - Controls over the preparation of the information, for example, controls over the preparation, review and maintenance of MIS reports, budgets, etc.

Analytical Procedures in the Overall Review at the End of the Internal Audit

15. **The internal auditor should apply analytical procedures at or near the end of the internal audit when forming an overall conclusion as to whether the systems, processes and controls as a whole are robust, operating effectively and are consistent with the internal auditor's knowledge of the business.** The conclusions drawn from the results of such procedures are intended to corroborate conclusions formed during the internal audit of individual components or elements of the financial statements, e.g., purchases, and assist in arriving at the overall conclusion. However, in some cases, as a result of application of analytical procedures, the internal auditor may identify areas where further procedures need to be applied before the internal auditor can form an overall conclusion about the systems, processes and associated controls.

Extent of Reliance on Analytical Procedures

16. The application of analytical procedures is based on the expectation that relationships among data exist and continue in the absence of known conditions to the contrary. The presence of these relationships provides the internal auditor evidence as to the completeness, efficiency and effectiveness of systems, processes and controls. However, reliance on the results of analytical procedures will depend on the internal auditor's assessment of the risk that the analytical procedures may identify relationships as expected when, in fact, a material misstatement exists.
17. The extent of reliance that the internal auditor places on the results of analytical procedures depends on the following factors:
- materiality of the items involved, for example, when inventory balances are material, the internal auditor does not rely only on analytical procedures in forming conclusions. However, the internal auditor may rely

solely on analytical procedures for certain income and expense items when they are not individually material;

- other internal audit procedures directed toward the same internal audit objectives, for example, other procedures performed by the internal auditor while reviewing the credit management process, in the collectibility of accounts receivable, such as the review of subsequent cash receipts, might confirm or dispel questions raised from the application of analytical procedures to an ageing schedule of customers' accounts;
- accuracy with which the expected results of analytical procedures can be predicted. For example, the internal auditor will ordinarily expect greater consistency in comparing gross profit margins from one period to another than in comparing discretionary expenses, such as research or advertising; and
- assessments of inherent and control risks, for example, if internal control over sales order processing is weak and, therefore, control risk is high, more reliance on tests of details of transactions and balances than on analytical procedures in drawing conclusions on receivables may be required.

18. The internal auditor will need to consider testing the controls, if any, over the preparation of information used in applying analytical procedures. When such controls are effective, the internal auditor will have greater confidence in the reliability of the information and, therefore, in the results of analytical procedures. The controls over non-financial information can often be tested in conjunction with tests of accounting-related controls. For example, an entity in establishing controls over the processing of sales invoices may include controls over the recording of unit sales. In these circumstances, the internal auditor could tests the controls over the recording of unit sales in conjunction with tests of the controls over the processing of sales invoices.

Investigating Unusual Items or Trends

19. When analytical procedures identify significant fluctuations or relationships that are inconsistent with other relevant information or that deviate from predicted amounts, the internal auditor should investigate and obtain adequate explanations and appropriate corroborative evidence. The examination and evaluation should include inquiries of management and the application of other auditing procedures until the internal auditor is satisfied that the results or relationships are sufficiently explained. Unexplained results or relationships may be indicative of a significant condition such as a potential error, irregularity, or illegal act. Results or relationships that are not sufficiently explained should be communicated to the appropriate levels of management. The internal auditor may recommend appropriate courses of action, depending on the circumstances.
20. The investigation of unusual fluctuations and relationships ordinarily begins with inquiries of management, followed by :
- corroboration of management's responses, for example, by comparing them with the internal auditor's knowledge of the business and other evidence obtained during the course of the internal audit; and
 - consideration of the need to apply other internal audit procedures based on the results of such inquiries, if management is unable to provide an explanation or if the explanation is not considered adequate.

Effective Date

21. This Standard on Internal Audit is applicable to all internal audits commencing on or after _____. Earlier application of the SIA is encouraged.

APPENDIX IX

STANDARD ON INTERNAL AUDIT (SIA) 7 QUALITY ASSURANCE IN INTERNAL AUDIT

CONTENTS

	Paragraph(s)
Introduction	1-2
Scope	3
Objective	4-10
Internal Quality Reviews	11-14
External Quality Review	15-17
Effective Date.....	18

The following is the text of the Standard on Internal Audit (SIA) 7, *Quality Assurance in Internal Audit*, issued by the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the “*Preface to the Standards on Internal Audit*”, issued by the Institute of Chartered Accountants of India.

In terms of the decision taken by the Council of the Institute taken at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as notified by the Council.

Introduction

1. Paragraph 3.1 of the *Preface to the Standards on Internal Audit*, describes the internal audit as follows:

“Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system. Internal audit, therefore, provides assurance that there is transparency in reporting, as a part of good governance.”

2. Paragraphs 7 and 8 of the Standard on Internal Audit (SIA) 2, Basic Principles Governing Internal Audit, state as follows:

“7. The internal auditor should either have or obtain such skills and competence, acquired through general education, technical knowledge obtained through study and formal courses, as are necessary for the purpose of discharging his responsibilities.

8. The internal auditor also has a continuing responsibility to maintain professional knowledge and skills at a level required to ensure that the client or the employer receives the advantage of competent professional service based on the latest developments in the profession, the economy, the relevant industry and legislation.”

Scope

3. This Standard on Internal Audit shall apply whenever an internal audit is carried out, whether carried out by an in house internal audit department or by an external firm of professional accountants. For the purpose of this Standard, the term “firm” means a sole practitioner/ proprietor,

partnership or any such entity of professional accountants as may be permitted by law¹.

Objective

4. The purpose of this Standard on Internal Audit (SIA) is to establish standards and provide guidance regarding quality assurance in internal audit.
5. **A system for assuring quality in internal audit should provide reasonable assurance that the internal auditors comply with professional Standards, regulatory and legal requirements, so that the reports issued by them are appropriate in the circumstances.**
6. **In order to ensure compliance with the professional Standards, regulatory and legal requirements, and to achieve the desired objective of the internal audit, a person within the organization should be entrusted with the responsibility for the quality in the internal audit, whether done in – house or by an external agency.**
7. **In the case of the in – house internal audit or a firm carrying out internal audit, the person entrusted with the responsibility for the quality in internal audit should ensure that the system of quality assurance include policies and procedures addressing each of the following elements:**
 - a) ***Leadership responsibilities for quality in internal audit* - The person entrusted with the responsibility for the quality in internal audit should take responsibility for the overall quality in internal audit.**

¹ The Standard on Quality Control (SQC) 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services Engagements* issued by the Council of the Institute of Chartered Accountants of India applies to the firms carrying out internal audit to the extent such internal audit activities fall under the scope of audits and reviews of the historical financial information and other assurance and other related services.

- b) ***Ethical requirements*** - The person entrusted with the responsibility for the quality in internal audit should establish policies and procedures designed to provide it with reasonable assurance that the personnel comply with relevant ethical requirements. If matters come to his attention that indicate that the members of the internal audit engagement team have not complied with relevant ethical requirements, he should, in consultation with the appropriate authority in the entity, determine the appropriate course of action.
- c) ***Acceptance and continuance of client relationship and specific engagement, as may be applicable***– The person entrusted with the responsibility for the quality in internal audit should establish policies and procedures for the acceptances and continuance of client relationships and specific engagements, designed to provide reasonable assurance that it will undertake or continue relationships and engagements.
- d) ***Human resources*** - The person entrusted with the responsibility for the quality in internal audit should establish policies and procedures regarding assessment of the staff's capabilities and competence designed to provide it with reasonable assurance that there are sufficient personnel with the capabilities, competence, and commitment to ethical principles necessary to:
 - Perform engagements in accordance with professional standards and regulatory and legal requirements; and
 - Enable the firm or engagement partner to issue reports that are appropriate in the circumstances.
- e) ***Engagement performance***– The person entrusted with the responsibility for the quality in internal audit should establish policies and procedures designed to provide it with reasonable assurance that

engagements are performed in accordance with the applicable professional Standards and regulatory and legal requirements and that the reports issued by the internal auditors are appropriate in the circumstances.

- f) **Monitoring** - The person entrusted with the responsibility for the quality in internal audit should establish policies and procedures designed to provide reasonable assurance that the policies and procedures relating to the system of quality assurance are relevant, adequate, operating effectively and complied with in practice.
8. In order to improve the functionalities of the organisation, transparency in reporting and good governance, the person entrusted with responsibility for the quality in internal audit, while establishing the quality assurance framework, should consider the following parameters of the internal audit activity:
- Terms of engagement and their adequacy.
 - Professional standards and compliance therewith.
 - Internal audit goals and the extent to which they are being achieved.
 - Recommendations for improving the quality of internal audit and the extent to which they are being implemented and their effectiveness.
 - Skills and technology used in carrying out internal audit.
9. The person entrusted with the responsibility for the quality in internal audit needs to ensure that the quality assurance framework is embedded in the internal audit. This can, for example, be achieved in the following manner:
- Developing an internal audit manual clearly defining the specific role and responsibilities, policies and

procedures, documentation requirements, reporting lines and protocols, targets and training requirements for the staff, internal audit performance measures and the indicators.

- Ensuring that the internal audit staff at all levels is appropriately trained and adequately supervised and directed on all assignments.
- Identifying the customers of the internal audit activity.
- Establishing a formal process of feedback from the users of the internal audit services, such as the senior management executives, etc. Some of the attributes on which the feedback may be sought include quality, timeliness, value addition, efficiency, innovation, effective communication, audit team, time management. **The responses received from the users of the internal audit services should also be shared with the appropriate levels of management and those charged with governance.**
- **Establishing appropriate performance criteria for measuring the performance of the internal audit function. In case the internal audit activity is performed by an external agency, the contract of the engagement should contain a clause for establishment of performance measurement criteria and periodic performance review. These performance measurement criteria should be approved by the management.**
- Identify and benchmark with industry/ peer group performance.

10. The quality assurance framework established by the person entrusted with the responsibility for the quality in internal audit should, therefore, cover all the elements of the internal audit activity. For example,

- Development and implementation of the internal audit policies and procedures.

- Maintenance and monitoring of the budget for the internal audit activity.
- Maintenance and updations of the overall internal audit plan.
- Identification of the risk areas and the internal audit plan to address these risks.
- Acquisition and deployment of audit tools and use of technology to enhance the efficiency and effectiveness of the internal audit activity.
- Co-ordination with the external auditors.
- Staffing related aspects of internal audit – recruitment, training, etc.
- Planning and implementation of the training and professional development of the internal audit staff.
- Implementation of the performance metrics for the internal audit activity and periodic monitoring of the same.
- Review of the follow up actions taken on the findings of the internal audit activity.

Internal Quality Reviews

- 11. The internal quality review framework should be designed with a view to provide reasonable assurance to that the internal audit is able to efficiently and effectively achieve its objectives of adding value and strengthening the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system.**

Internal Quality Reviewer

- 12. The internal quality review should be done by the person entrusted with the responsibility for the quality in**

internal audit and/ or other experienced member(s) of the internal audit function.

13. The internal quality reviews should be undertaken on an ongoing basis. The person entrusted with the responsibility for the quality in internal audit should ensure that recommendations resulting from the quality reviews for the improvements in the internal audit activity are promptly implemented.

Communicating the Results of the Internal Quality Review

14. The person entrusted with the responsibility for the quality in internal audit should also ensure that the results of the internal quality reviews are also communicated to the appropriate levels of management and those charged with governance on a timely basis along with the proposed plan of action to address issues and concerns raised in the review report.

External Quality Review

15. External quality review is a critical factor in ensuring and enhancing the quality of internal audit. **The frequency of the external quality review should be based on a consideration of the factors such as the maturity level of the internal audit activity in the entity, results of the earlier internal audit quality reviews, feedbacks as to the usefulness of the internal audit activity from the customers of the internal audit, costs *vis a vis* perceived benefits of the frequent external reviews. The frequency should not in any case be less than once in three years.**

External Quality Reviewer

16. The external quality review should be done by a professionally qualified person having an in depth knowledge and experience of, inter alia, the professional Standards applicable to the internal auditors, the processes and procedures involved in the internal audit generally and those peculiar to the industry in which the entity is operating, etc. The external quality reviewer

should be appointed in consultation with the person entrusted with the responsibility for the quality in internal audit, senior management and those charged with governance.

Communicating Results of the External Quality Review

17. The external quality reviewer should discuss his findings with the person entrusted with the responsibility for the quality in internal audit. His final report should contain his opinion on all the parameters of the internal audit activity, as discussed in paragraph 10, and should be submitted to the person entrusted with the responsibility for the quality in internal audit and copies thereof be also sent to those charged with governance. The person entrusted with the responsibility for the quality in internal audit should, also submit to those charged with governance, a plan of action to address the issues and concerns raised by the external quality reviewers in his report.

Effective Date

18. This SIA is effective for all quality assessments/ reviews of internal audit undertaken on or after
Earlier application of the SIA is encouraged.

APPENDIX X

STANDARD ON INTERNAL AUDIT (SIA) 8 TERMS OF INTERNAL AUDIT ENGAGEMENT

CONTENTS

	Paragraph(s)
Introduction.....	1-2
Terms of Engagement	3
Elements of Terms of Engagement.....	4-22
<i>Scope</i>	5-9
<i>Responsibility</i>	10-13
<i>Authority</i>	14-15
<i>Confidentiality</i>	16-18
<i>Limitations</i>	19
<i>Reporting</i>	20
<i>Compensation</i>	21
<i>Compliance with Standards</i>	22
Withdrawal from the Engagement	23
Effective Date	24

The following is the text of the Standard on Internal Audit (SIA) 8, *Terms of Internal Audit Engagement*, issued by the Institute of Chartered Accountants of India. The Standard should be read in the conjunction with the “*Preface to the Standards on Internal Audit*”, issued by the Institute.

In terms of the decision taken by the Council of the Institute at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as may be notified by the Council in this regard.

Introduction

1. The purpose of this Standard on Internal Audit is to establish standards and provide guidance in respect of terms of engagement of the internal audit activity whether carried out in house or by an external agency. A clarity on the terms of the internal audit engagement between the internal auditors and the users of their services (hitherto known as “*auditee*”) is essential for inculcating professionalism and avoiding misunderstanding as to any aspect of the engagement.
2. **The internal auditor and the auditee should agree on the terms of the engagement before commencement.** The agreed terms would need to be recorded in an engagement letter. Normally, it is the responsibility of the internal auditor to prepare the engagement letter and it is to be signed both by the internal auditors as well as the auditee.

Terms of Engagement

3. The terms of engagement of the internal audit, *inter alia*, define the scope, authority, responsibilities, confidentiality, limitation and compensation of the internal auditors. **The terms of engagement should be approved by the Board of Directors² or a relevant Committee thereof such as the Audit Committee or such other person(s) as may be authorised by the Board in this regard. The terms should be reviewed by the internal auditor and the audit committee periodically and modified suitably, if required, to meet the changed circumstances.**

Elements of Terms of Engagement

4. The following are the key elements of the terms of the internal audit engagement:
 - i. Scope
 - ii. Responsibility

² Or an equivalent authority where the entity is not in a corporate form. For example, the Board of Trustees in a cooperative society.

- iii. Authority
- iv. Confidentiality
- v. Limitations
- vi. Reporting
- vii. Compensation
- viii. Compliance with Standards

Each of these elements has been discussed in the following paragraphs.

Scope

- 5. Paragraph 3.1 of the Preface to the Standards on Internal Audit describes internal audit as *“an independent function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system.”*
- 6. **The terms of the engagement should contain a statement in respect of the scope of the internal audit engagement. It should clearly delineate the broad areas of function of internal audit like evaluating internal controls, review of business process cycle controls, risk management and governance.**
- 7. **It should indicate areas where internal auditors are expected to make their recommendations and value added comments.**
- 8. **The terms of engagement should clearly mention that the internal auditor would not, ordinarily, be involved in the preparation of the financial statements of the auditee. It should also be made clear that the internal audit would not result in the expression, by the internal auditor, of an opinion, or any other form of assurance on the financial statements or any part thereof of the auditee.**

9. **The scope of the terms of the engagement, after delineating the broad areas of function of internal audit, should clarify that any additional services that are not encompassed by the engagement letter shall be performed only on mutual agreement and with separate engagement letter.**

Responsibility

10. **The terms of the engagement should clearly mention the responsibility of the auditee vis a vis the internal auditor.** The auditee is responsible for establishing, maintaining and ensuring operating effectiveness of a system of internal control. The auditee would also be responsible for timely communication of material weaknesses or other significant issues relating to internal controls, misstatements in the financial information or similar matters to its external auditors, the Audit Committee, the Board of Directors, regulators and to those to whom the auditee is required to so communicate.
11. The management of the auditee is responsible for providing timely and accurate data, information, records, personnel etc., and for extending cooperation to the audit team.
12. **Similarly, where the internal auditor has a specific responsibility, say that arising out of a law or a regulation or a professional standard applicable to the internal auditor, to communicate directly, the above mentioned issues to an appropriate authority or someone within the entity or a regulator, the terms of the engagement should contain a clear mention of such responsibility.**
13. The internal auditor has the responsibility to inform the management before commencement of the assignment about the engagement team and the audit plan.

Authority

14. **The terms of engagement should provide the internal auditor with requisite authority, including unrestricted access to all departments, records, property and personnel and authority to call for information from concerned personnel in the organisation.**

15. The internal auditor should have full authority on his technologies and other properties like hardware and audit tools he may use in course of performing internal audit.

Confidentiality

Confidentiality of Working Papers

16. The terms of engagement should be clear that the ownership of the working papers rests with the internal auditor and not the auditee. It should also be made clear that the internal auditor may, upon a request received in this regard from the auditee, provide copies of non proprietary working papers to the auditee. The terms should lay down the policy and the procedures to be followed regarding requests received for internal auditor's working papers from third parties including external auditors.
17. The internal audit engagement may also be subject to a peer review by a regulator, requiring the internal auditor to disclose his working papers to the peer reviewer without the permission of the auditee. **The engagement letter should bring out this fact clearly.**

Confidentiality of the Report

18. The engagement letter should contain a condition that the report of the internal auditor should not be distributed or circulated by the auditee or the internal auditor to any party other than that mutually agreed between the internal auditor and the auditee unless there is a statutory or a regulatory requirement to do so.

Limitations

19. The terms of engagement should specify clearly the limitations on scope, coverage and reporting requirement, if any. It may also mention that the internal auditor or any of his employees shall not be liable to the auditee for any claims, damages, liabilities or expenses

relating to the engagement exceeding the aggregate amount of compensation agreed upon by both the parties.

Reporting

20. The terms of the engagement should clearly lay down the requirements as to the manner frequency of reporting and the list of intended recipients of the internal audit report.

Compensation

21. There should be a clear understanding among the internal auditor and the client as to the basis on which the internal auditor would be compensated, including any out of pocket expense, taxes etc., for the services performed by him.

Compliance with Standards

22. The terms of the internal audit engagement should contain a statement that the internal audit engagement would be carried out in accordance with the professional Standards applicable to such engagement as on the date of audit.

Withdrawal from the Engagement

23. In case the internal auditor is unable to agree to any change in the terms of the engagement and/ or is not permitted to continue as per the original terms, he should withdraw from the engagement and should consider whether there is an obligation, contractual or otherwise, to report the circumstances necessitating the withdrawal to other parties.

Effective Date

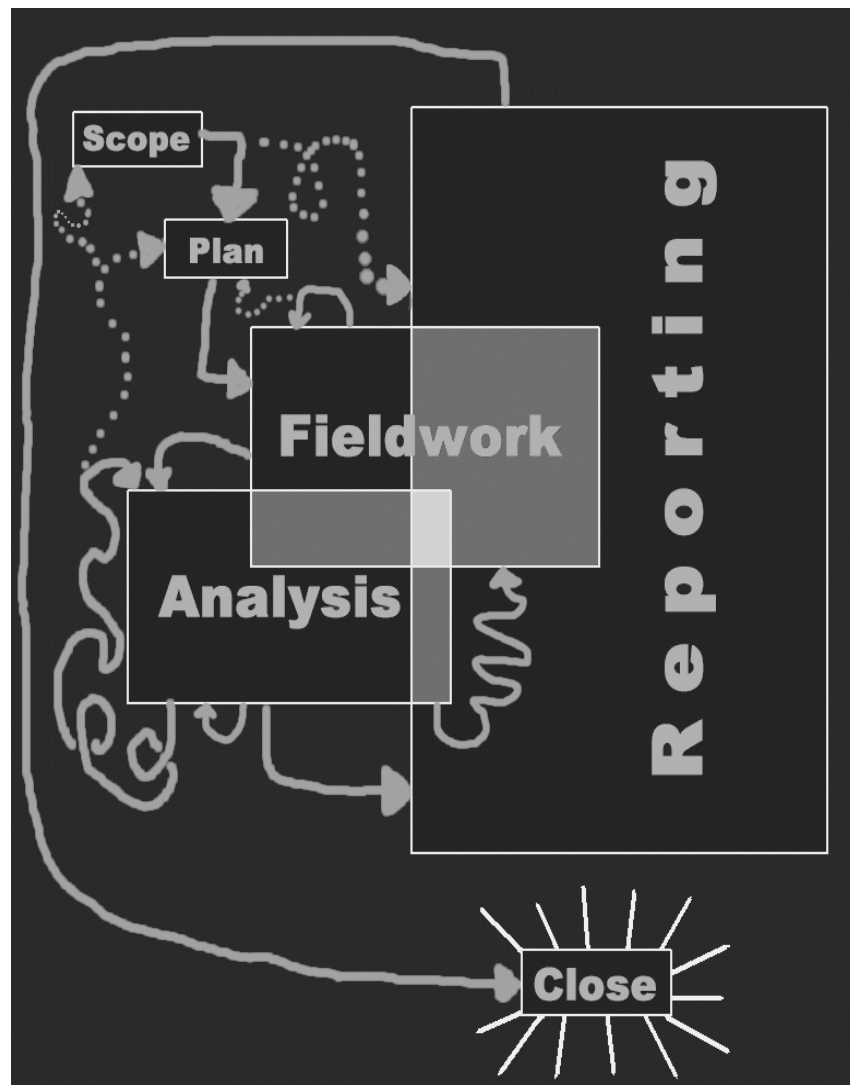
24. This Standard on Internal Audit is effective for all internal audits beginning on or after.....
Earlier application of the Standard is encouraged.

MODULE - III

MANAGING THE INTERNAL AUDIT ACTIVITY

Introduction to Internal Audit Engagement Management

Overview of the flow of Internal Audit
Engagement



Detailed Steps

Step- 1

- Determination of the Scope of the Internal Audit Engagement.

Step-2

- Understand the client's business.
- Understand the internal controls environment.
- Evaluation of the past internal audit report applicable to the scope of the engagement.
- Evaluate internal audit risk, using professional judgment.

Step 3

Perform preliminary analytical procedures to:

- Identify significant processes and controls structure.
- Highlight material risks and adverse relationships.
- Obtain sufficient audit assurance for reducing/eliminating detail testing.

Step- 4

- Formulation of the Basic Problem in light of the Scope of the Engagement.

Step- 5

- Plan for key transactions and controls to be tested.
- Identification of the Sampling Methodology.
- Determination of the Sample Population and Size.
- Determination of the risk element in the sample formulation i.e., Alpha – Risk of the Sample Methodology.

Step - 6

- Perform substantive analytical testing.
- Perform substantive tests of detail.

Step - 7

- Working papers to have adequate audit evidence.
- Complete lead schedules.
- Prepare internal audit summary memorandum.
- Review internal audit team findings.

Step – 8

- Final discussion points and issue resolution.
- Debriefing meetings with client/staff.
- Communicate control weaknesses to management.
- Draft internal audit report.

Chapter-III.2

Internal Audit Planning

Paragraph 3.1 of the *Preface to the Standards on Internal Audit* issued by the Institute describes Internal Audit as :

“Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto, and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system.”

Thus, in order to perform a critical appraisal of the functioning of an entity and to suggest improvements so as to strengthen the governance mechanism of the organization. The internal audit planning has to be well nested so that the meaningful result could be drawn with.

Why Internal Audit Planning

Standard on Internal Audit (SIA) 1, *Planning an Internal Audit* issued by the Institute amplifies the basic principles that the internal auditor should plan his work to enable him to conduct an effective internal audit in efficient and timely manner. Adequate planning ensures that appropriate attention is devoted to significant areas of audit, potential problems are identified and the skills and time of the staff are appropriately used.

Elements of Planning

- Developing an overall plan for the expected scope and conduct of internal audit; and
- Developing an audit program showing the nature timing and extent of audit procedures.

Scope of the Internal Audit

- Prepare a scoping document,
- Arrange a kick-off meeting with the key process owner / departmental head.

The scoping document contains the following :

- Objective- what the project aims to achieve,
- Scope- the magnitude and boundaries of activities, objectives and exposures to be reviewed,
- Proposed timeline for the completion of the work,
- Scoping document can also include the results from any previous internal audit or any other independent reviews, and
- Additional information on recent events may also be included in the scoping document.

Arrange a kick-off meeting with the key process owner,

- At the opening meeting we need to inform them about the scope, obtain their input and meet the various process owners.
- The key objective of this meeting is:
 - Manage the process owner's expectations.
 - Obtain the process owners acceptance and support for the process.
 - Identify additional work that the process owner may require.

Development of Internal Audit Resource

After determining the scope of Internal Audit it is necessary to estimate time and resources which are the necessary for the performing the Internal Audit.

- Estimation of time of the Internal Audit depends on the factors like Organisation Business Process i.e., centralized

Training Material on Internal Audit

or decentralized, Organization Culture, Degree of Specialization required and resource constraints.

- On the other hand the Estimation of the resources is directly propositioned to familiarity of the industrial processes, aptitude of the members and time factor of completion of the Internal Audit.

Once the team has been identified, carry out audit briefing, which includes:

- Communication of the timing for the completion of the Internal Audit.
- Assigning specific roles to be performed by the audit team members.
- Understanding the review processes and quality control measures that will be in place.
- Agreeing individual objectives for the audit to allow individual performance feedback against the competencies.

Steps Involved in Planning Process

Obtaining Knowledge of Business

The internal auditor should obtain a level of knowledge of the entity sufficient to enable him to identify events, transactions, policies and practices that may have a significant effect on the Internal Audit. Following are some of the sources wherefrom the internal auditor can obtain such knowledge:

- Previous experience, if any, with the entity and the industry.
- Legislation and regulations that significantly affect the entity.
- Entity's policy and procedures manual.
- Management reports/ internal audit reports of prior periods.
- Newspaper/ industry journals.

- Discussion with client's management and staff.
- Visits to entity's plant facilities etc., to obtain first hand information regarding the production processes of the entity.
- Visits to the entity's department where the accounting and other documents are generated, maintained, and the administrative procedures followed.
- Other documents produced by the entity, for example, material sent to the shareholders and the regulatory authorities, management policy manuals, manuals relating to accounting and internal controls, organizational charts, job description charts, etc.

Knowledge of the entity's business, among other things, helps the internal auditor to identify areas requiring special focus, evaluate the appropriateness of the accounting policies and disclosures, accounting estimates and management representations. Knowledge of the business would also help the auditor to identify the priorities of the business, critical factors or constraints in the smooth running of the business as also understand the trends in respect of various financial and operating ratios, etc.

Obtaining Knowledge of the Process

The process analysis helps the internal auditor in identifying the specific audit consideration as it helps him in evaluating the reasonableness of controls, systems and management representations so that the basic problem in line with the scope of the terms of the engagement can be formulated

- *The purpose of business process analysis performed in the initial stages of audit execution is to drive the content and focus of an internal audit program associated with an individual internal audit*
- *Potential benefits of business process analysis is to provide an assessment of the component processes*

and internal controls while providing information on comparative practices,

- *Performing process analysis allows for a structured and efficient way of identifying highly effective and valuable recommendations.*

Understanding the Process

We need to gain an understanding and document the process that we intend to audit:

- What information do we want?
- Why do we need this information?
- How do we get it?

Issues to consider in process analysis:

- Inputs to the process,
- Activities involved in carrying out the process,
- Outputs of the process,
- Technology interfaces, and
- People mapping,

Process analysis is the step in which we extend our understanding of processes. Process analysis consists of understanding and documenting the process, and is generally performed concurrently with process risk and control assessment. Process understanding is commonly performed through interviews and discussions. These discussions are typically conducted with those individuals who are intimately familiar with the process such as process owners or control owners.

Key Activities :

- Discuss in detail the process involved
 - What are the activities? → Initiation, Process capture.
 - Who performs the activity ?→ Approval
 - When are the activities documented? → Record, Post/Account
 - What tools/technology is used ?
- There should be two people involved during process interview, one for documenting the narrative and other for leading the interview.

Process understanding should be documented in narrative form and / or through the use of flowcharts to cover manual operations as well as computerized, inter-department/inter-location linkages.

It is important that we validate the flow charts/narratives we have prepared with process owner to ensure we have an accurate representation of the process. Ascertain fitment of process with regard to business objectives. Seek data/ supporting for validating the process, finally we need to conduct a design walkthrough.

Key Activities:

- ♦ Conducting a logical walkthrough,
- ♦ Process owner may sometimes inform what they think is the process and not what is the actual process,
- ♦ Checking whether the process is applicable for all transaction or there are some exceptions,
- ♦ Sticking to standards while preparing the narrative or process flows,

- ◆ Process mapping/narrative should be done immediately post interview to ensure that no data is forgotten, and
- ◆ Process flows/ Flowcharts are used to describe a complete process from start to end while narratives are used to describe only a part of the process.

Formulation of the Basic Problem in light of the Scope of the Terms of Engagement

The next stage in planning an internal audit is establishing the basic problem. The basic problem should be sufficient in coverage so as to meet the objectives of the engagement. The internal auditor should consider the information gathered during the preliminary review stage to determine the scope of his audit procedures. The nature and extent of the internal auditor's procedures would also be affected by the terms of the engagement. In case the internal auditor is of the view that circumstances exist which would restrict the auditor from carrying out the procedures, including any alternative procedures, considered necessary by him, he should discuss the matter with the client to reach a conclusion whether or not to continue the engagement. The basic problem should be documented comprehensively to avoid misunderstanding on the areas covered for audit. The internal auditors are often confronted with a situation where client denies access to certain information or has a negative list of areas where internal audit is not desired. There are also situations where while the client requires internal audit procedures to be carried but findings are not to form part of the report but to be reported separately.

Sample IA Plan

PROPOSED INTERNAL AUDIT PLAN FOR 2007	No of hrs	Type		
		Senior Manager	Manager	Asst. Manager
Quarter 1				
▪Sales order management (Revenue Assurance)	72	2	5	10
Quarter 2				
▪Procure to pay including inventory management:	140	5	15	20
▪Raw material purchases	165	10	25	30
▪Other purchases	180	15	35	40
Quarter 3				
▪Human Resources and payroll	165	5	15	20
▪Close of books process	180	10	25	30
▪Recruitment and separation	210	15	35	40
▪Security	165	5	15	20
▪Third party process efficiency	175	10	15	20
▪Payroll	150	15	20	25
Quarter 4				
▪Treasury and forex	120	10	15	20
▪Production planning	180	10	25	30
▪Waste disposal	180	20	30	40
▪IT Security	120	10	15	15
▪New product development	135	15	20	15
▪MIS and P & L reconciliation	130	10	20	20

Chapter-III.3

Internal Audit Program

The internal auditor should also prepare a formal internal audit programme listing the procedures essential for meeting the objective of the internal audit plan. Though the form and content of the audit programme and the extent of its details would vary with the circumstances of each case, yet the internal audit programme should be so designed as to achieve the objectives of the engagement and also provide assurance that the internal audit is carried out in accordance with the Standards on Internal Audit. As a corollary, the audit plan developed by the internal auditor would need to be a risk-based plans, appropriately reflecting and addressing the priorities of the internal audit activity, consistent with the organisation's goals. The internal audit programme should also be finalised in consultation with the appropriate authority before the commencement of the work.

The internal audit programme identifies, in appropriate details :

- the objectives of the internal audit in respect of each area,
- the staff responsible for carrying out the particular activity,
- the time allocated to each activity as also the sufficiently detailed, and
- Sufficiently detailed instructions to the staff as to how to carry out those procedures.

The internal audit programme may also have provision for information such as:

- the procedures actually performed,
- reasons for not performing the originally identified procedures,
- actual time consumed in carrying out the relevant procedure, and

- reasons for deviations from budgeted time etc.

A well prepared, comprehensive audit programme helps proper execution of the work as well as of the proper supervision, direction and control of the performance of the engagement team.

Sample- Information requisition

Description of Information/Data

- ◆ Copy of existing process flow charts, operating procedures and policies including specifically the following:
 - a. Schedule of authority for expense and payments.
 - b. User manual and process flows used for Oracle.
 - c. Valid circulars/ mails on policies.
- ◆ Summary of active projects - Project Description, Nature of Project (commercial/ residential), Location, Project Size (Budget, Duration), Current Completion status, Project Head etc.
- ◆ Details of management review committees (Composition, Role, Responsibilities, Frequency of meetings, Agenda, Minutes of meeting for last 1 year etc)
- ◆ Copies of internal audit reports/ management audit reports for last 2 years.
- ◆ Copy of Information presented to the Board as part of the Board Agenda (last two months) and copy of Minutes of the meetings (Board, Audit Committee and Executive Committee if any) for last two years.
- ◆ Summary of agreements with main service providers and business associates
- ◆ Copies of existing statutory and legal compliance checklists and procedures

Training Material on Internal Audit

- ◆ Listing of existing MIS Reports by Function/ Company as a whole (Daily/ Weekly/ Monthly/ Quarterly) and copy for last 3 consecutive months
- ◆ Details of IT Applications currently in use as follows:
 - Name of the application
 - Purpose of the application
 - Integrated with main financial application - yes / no, (if no is it proposed to be integrated - yes / no)

Sample Audit Program Document

S No	Areas / Processes	Remarks / Particulars – sample, criteria for selection, timelines, audit in-charge etc
1	Purchase procedure: <ul style="list-style-type: none">➤ vendor registration, evaluation, appraisal➤ SOA➤ Dependence on supplier	
2	Inventory / Materials Management: <ul style="list-style-type: none">➤ Receipts, issue, balance➤ PV➤ Valuation➤ Rising component cost	

S No	Areas / Processes	Remarks / Particulars – sample, criteria for selection, timelines, audit in-charge etc
3	Repairs: <ul style="list-style-type: none">➤ Rate fixation➤ Cause analysis➤ Emergency repair team	
4	Maintenance: <ul style="list-style-type: none">➤ Preventive➤ Shutdown	
5	Fixed Assets Management: <ul style="list-style-type: none">➤ identification➤ record keeping➤ insurance➤ PV	
6	Goods returned	
7	Legal expenses	
8	Year end adjustments	
9	Liquidated Damages	
10	Marketing: <ul style="list-style-type: none">➤ Ad-spend	

Training Material on Internal Audit

S No	Areas / Processes	Remarks / Particulars – sample, criteria for selection, timelines, audit in-charge etc
	<ul style="list-style-type: none"> ➤ Market intelligence ➤ MIS 	
11	Production and plant operations: <ul style="list-style-type: none"> ➤ Calibration/ weighbridge ➤ Production planning and scheduling ➤ PC committee meetings 	
12	IT systems	
13	HR and Payroll	
14	Statutory compliance	
15	Safety Health Environment	
16	Scrap generation Third Party Transfers/ repairs	
17	Expenses (Budget vs Actuals)	
18	DN / CN	
19	Sales: <ul style="list-style-type: none"> ➤ Credit management ➤ debtors ageing ➤ non / slow moving items 	

S No	Areas / Processes	Remarks / Particulars – sample, criteria for selection, timelines, audit in-charge etc
	<ul style="list-style-type: none">➤ Debtors Turnover ratio➤ Receivables monitoring➤ Disc Policy➤ Pricing➤ Dealership appointment and control	
20	Knowledge Management / Portal	
21	Logistics and Supply Chain Management	
22	Product Warranty costs and provisioning – AS 29	
23	Energy conservation	
24	IPR – Patents and Trademarks	
25	Risk Management – IA review	
26	MIS Reporting	

Chapter-III.4

Documentation

Purpose of documentation is to:

- Assist in planning, performing, supervising, and reviewing the engagement.
- Collect important client and engagement material in one location.
- Provide a record of principal judgments and the evidential matter obtained to support conclusions, findings, and recommendations in the final report.
- Assist reviewers in understanding the work performed.
- Provide evidence that the internal audit work is performed in accordance with the scope of work as mentioned in engagement letter, Standards on Internal Audit (SIAs) and other relevant pronouncements issued by the ICAI.

Internal Audit Documentation should record:

- Internal Audit Charter or Engagement Letter, as the case may be.
- Internal Audit Plan.
- The nature, timing and extent of audit procedures performed.
- The conclusion drawn.

Chapter-III.5

Sampling in Internal Audit

The Internal auditor should design and select an audit sample to perform audit procedures and evaluate sample results.

Key steps in the construction and selection of a Sample include:

- Determine the objectives of the internal audit.
- Define the population to be sampled.
- Determine the sampling methods.
- Calculate the sample size.
- Select the sample.

Note : Evaluate the sample from an audit perspective.

Sampling Techniques

There are two general approaches to audit sampling:

- Statistical Sampling- is an objective method of determining the sample size and selection criteria. Here, the auditor quantitatively decides how closely the sample should represent the population and the number of times in 100 the sample should represent the population.
- Non-Statistical Sampling or judgmental sampling- here the decisions are based on subjective judgment as to which items/transactions are the most material and most risky.

Statistical Sampling Techniques

Sampling can help to reach a statistically valid conclusion about a data population from a relatively small number of samples. There are two common sampling techniques:

- Monetary unit sampling (MUS), in which the population consists of the absolute value of a numeric field.
- Transaction sampling, also called record sampling, in which the population consists of the number of records.

Statistical Sampling

The three different methods for selecting the items in the sample:

- Fixed-interval- In fixed-interval sampling, auditors specify a selection interval. Fixed interval is used for sample selection. A decidedly nonrepresentative sample can be drawn if the data has a pattern that coincides with the interval one specifies.
- Cell, also known as random interval- Sample for testing is selected in random interval. The main advantage of this is that it automatically avoids problems relating to patterns in the data. A disadvantage is that the entries selected in cell sampling might not be as consistent as those selected in fixed-interval sampling.
- Random-If one uses random sampling, the internal audit need to be aware that while each item has an equal chance of selection, there is no guarantee that the results will be evenly distributed.

Sampling and CAATS

- The internal auditor can also use computer assisted audit techniques (CAATs)- In case where statistical sampling approach is required, use of software tools such as IDEA, ACL or Microsoft Access can significantly increase our coverage for a given level of effort and help focus our efforts

on areas where the internal audit are more likely to find results.

- CAATS offers the following advantages:
 - Reduced level of audit risk.
 - Broader and more consistent audit coverage.
 - Faster availability of information.
 - Improved exception identification.
 - Greater opportunity to quantify internal control weaknesses.
 - Cost savings over time.

Chapter-III.6

Risk Assessment and Internal Controls

Risk Factors – an Illustration

Business Objectives	External Risk Factors	Internal Risk Factors
Financial performance	Macro economy	Financial reporting risks
Client and Market focus	Political environment	Liquidity
Execution excellence	Forex exchange transactions	Intellectual Property management
Organization and Development	Revenue concentration	HR management
	Technological obsolescence	Legal compliance
	Security and business continuity	Engagement execution
		Culture and values

Risk Assessment Template – Illustrative

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

Risk Values

Cause	Risk Impact	Potential Loss (Rs. Crore)	Probability	Control Effectiveness	Residual Risk Value (Rs. Crore)
Service delivery failure	Reputation	4	1.0 (High)	Strong (0.75)	1
Wrong financial plan and budget	Cost over run	3	0.5 (Medium)	0.5 (Medium)	0.75
Inadequate systems functionality	Infrastructure failure	5	0.25 (low)	Weak (0.25)	0.9375

Risk Assessment Techniques include –

Qualitative Techniques	Quantitative Techniques
1) Questionnaire	1) Probability based
2) Surveys	2) Back testing
3) Interviews	3) Sensitivity Analysis
	4) Scenario Analysis

Process Risk and Control Assessment

Key Activities:

- Identify Standard business risks.
- ‘What if analysis’ or ‘what can go wrong’ – Gross risk identification.
- Identify mitigating controls, if any.
- Identify non-value add, iterative and duplicate activities in process.
- Adopt ‘Lateral Thinking’ approach to challenge approaches followed for executing business activities.
- Identify areas for business improvement opportunities, if any.
- Document the identified risk and control into a Risk and Control Matrix (RCM).

Process Risk Assessment:

- Identify standard risk affecting the process.
- Trigger of risk occurring:
- Absence of documented processes.

- Change in key personnel.
- Significant growth in business when processes are not scalable.
- High magnitude of manual process.
- Change in the company structure.
- Key personnel leaving the organisation.

What-if Analysis

- What if analysis is a brainstorming approach that uses broad, loosely structured questioning to:
 - Postulate potential upsets that may result in accidents or system performance problems
 - Ensure that appropriate safeguards against those problems are in place
- Typically performed by one or more teams with diverse backgrounds and experience.
- Applicable to any activity or system.
- Generates qualitative descriptions of potential problems, in the form of questions and responses, as well as lists of recommendations for preventing problems.

Process Control Assessment

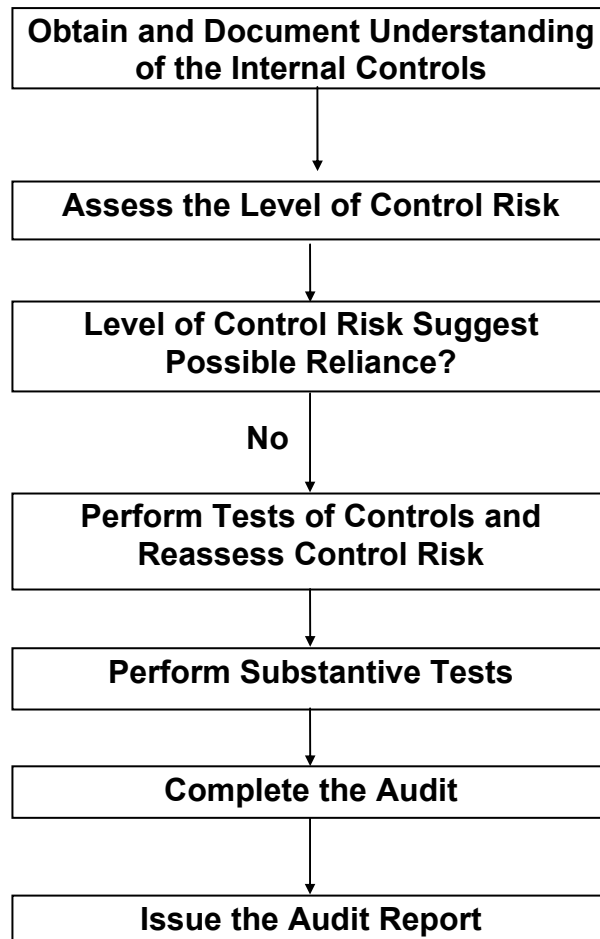
- Identify mitigating controls, if any.
- Identify and document control for each identified risk.
- Nature of Controls:
 - It should be specific and can be tested.
 - The control should be able to be evidenced.

Training Material on Internal Audit

- The control should be time-bound.
- Documentation of controls must:
 - Specify the risk it is addressing.
 - Describe the control.
 - State who performs the control.
 - State the evidence produced.

Compliance Vs. Substantive Approach in Internal Audit

Compliance and Substantive Approaches



Internal Auditor May Adopt Compliance Approach or Substantive Approach or A Combination of Both.

Compliance Approach

- The compliance approach is to assess whether proper control procedures have been established by the entity.
- Auditee entity should have procedures and documentation sufficient to cover each of the key control areas.

Substantive Approach

A substantive approach will be employed if the internal auditor chooses not to place reliance on the entity unit's specific controls or is of the opinion that the standard of robustness of systems and general compliance is not satisfactory. This approach requires an indepth review.

Control Testing

The requirements of internal audit testing:

- Internal audit work needs to be focused on the areas of highest value.
- Audit work performed must be sufficient to justify the conclusions being reached as a result of the audit.
- Audit work must be documented to support and evidence the conclusions being reached.
- Review and challenge of audit findings is key in delivering an insightful and comprehensive internal audit assignment.
- Testing needs to be sufficient to :
 - Come to a conclusion about the effectiveness of the control.
 - Allow the process owner to accept the findings.

Compliance Vs. Substantive Approach in Internal Audit

- Meet any regulatory requirements.
- Identify controls for testing,
- Select method of testing
 - Test of Design,
 - Test of effectiveness,
- Select Sample for testing.
- Validate the control to Identify Issues/ Gaps / Control weakness.
- If adverse observations are made – check for need to increase sample size.
- Perform root cause analysis.
- Confirm issues with Process Owners.
- Recommend mitigation plans.
- Summarise findings and performance improvement observations.

Identify Controls For Testing

Key Activities are:

- Define scope of testing and develop a testing plan,
- Identify key controls to test,
- Controls can be tested based on the nature of the control and the type of control,
- In selecting controls, it is efficient to consider first the controls that management routinely applies to monitor the achievement of the entity's objectives and to mitigate the impact of business risks,
- When determining the extent of tests to perform, assess:

Training Material on Internal Audit

- The nature of the control (manual controls should be subject to more extensive testing than automated controls);
- The frequency of operation of the control (the more frequent a manual control operates, the more operations of the control should be tested); and
- The importance of the control (controls that are relatively more important should be tested more extensively).

There are two types of internal audit procedures:

- Tests of Design is to evaluate the control design to ensure that design is robust to manage or mitigate the risk in a complete and comprehensive manner. To test design we take one transaction for each type of activity and trace it through each control step and activity.
- Tests of effectiveness confirms whether key internal controls identified during business process analysis are in existence and are operating as intended. To test effectiveness we select a sample of transaction to test whether they follow the design in consistent manner.

Test of Design Effectiveness

The procedures used to test the design of controls include:

- The inspection of documents and records.
- Inquiries of appropriate personnel in the entity.
- Walkthroughs of significant classes of transactions.

While testing the design of controls, the internal auditor considers:

- The risks it helps to mitigate,
- Frequency,
- Competence/experience of the person performing it (if manual control),

- The balance of controls in terms of preventive and detective; manual and automated; and also among the defined control categories.

Test of Operating Effectiveness

- Determines whether the control is operating as designed and performed by a person who possesses the necessary authority and qualifications to perform the control effectively.
- Techniques to determine the effectiveness of the operation of controls include:
 - Observation – of the performance of the control (e.g. physical verification of stock).
 - Inquiry – from process owner about the operation of a control.
 - Inspection – of records or documents supporting the operation of a control.
 - Re-performance – of the operation of a control to ascertain it's performance.
- Data analysis is commonly used in internal audit to validate operating efficiency in order to:
 - Verify completeness and accuracy of transactions (actual number and value vs should be number and value).
 - Identify abnormal trends, patterns and gaps reflecting indicators for process gaps/ risks.
- Other techniques, which represent a bundling of the above techniques are knowledge assessment, third party confirmations, corroborative enquiry and system query.

Sample Testing

Sampling and substantive verification include the following:

- Obtain details about universe of transaction.

Training Material on Internal Audit

- Define sample (use of sampling techniques) to ensure it covers adequate period and all categories.
- Conduct field work.
- If adverse observations are made, check for need to increase sample size.
- List preliminary observations and discuss with process owners.

Quality Control – Internal Audit issues

- quality is built into the process rather than relying on post-production audits or checklists;
- responsibilities for each engagement team member in the control process are clearly defined and properly communicated;
- controls respond to key risks in a timely manner. Too many controls results in no control;
- controls are built in a cascade, with an appropriate mix of external, group, team and individual controls;
- controls are results-focussed; and
- process owners participate in the continuous evolution of the control framework.

Chapter-III.8

Issue Resolution and Obtaining Management Comments

Internal Audit Issues Discussion

Audit finding:- A finding is noted when the testing of controls highlights that a high residual risk remains.

The controls tested are either:

- Not operating as intended (tests of effectiveness),
- Are ineffective at reducing risk (test of design),

Once testing has been completed it is necessary to :

- Confirm the issues raised with the process owner – To ensure the audit team have not misinterpreted issues and confirm findings for factual accuracy,
- It is also important to ensure that the process owner does not have any “surprises” when presented with the internal audit report,
- Agree, in outline, the recommendation proposed and develop with the process owner an action plan to address the weaknesses and/or gaps in the control environment.

Recommend Mitigation Plans

Based on impact and identified root causes, bifurcate identified risks based on level of effort required to counter risks through change/ establishment of controls:

- Can be countered immediately – minor changes in processes with no/ minimal system changes,

Training Material on Internal Audit

- Can be countered in short term – reasonable changes in key activities within a process along with change in system configurations, and
- Can be countered in long term – significant investments involving process redesigning, system upgradation etc.

Based on discussions with process owners understand the mitigation level that the management wants to achieve for every identified risk.

Formulate recommendations to mitigate the identified risks by suggesting improvements in process and internal control designs and obtain management's buy-in on the same.

Internal Audit Execution

Summaries, Findings and Performance Improvement Observations

A finding is noted when the results of internal control testing denotes that the control is either missing or not working as expected and is to be documented on the summary of findings. All findings included in the internal audit report should tie back to the summary of finding which in turn should tie directly back to the supporting test documentation or other relevant workpapers. Performance improvement observation is defined as an area for improvement that does not involve a control weakness.

Based on the results of performing the audit work, as contained in the audit programme, we document:

- The audit work performed and the results gathered.
- The basis for our observation/finding.
- The risk to the organisation as the control is not working as intended.
- A recommendation to upgrade the system/process to plug the gap in control.
- Management's response to our findings and recommendations.

Internal Audit Reporting

Objective of Reporting and Follow-up

The primary objective of an internal audit report is to effectively communicate the results of the audit. Thereby ensuring that the report:

- Assists process owners in improving their operations and controls.
- Is used as a management tool.
- Helps bring about improvement in the organisation.
- Contributes to the achievement of the overall business objectives.
- Leads to improved performance and control framework.
- The follow-up process monitors the progress of agreed upon management action plans and reports this progress to senior management and the audit committee.

Internal Audit Issues Resolution

The follow-up process monitors the progress of agreed-upon management action plans and reports this progress to senior management and the audit committee. Follow-up is often overlooked but it is one of the most important stages of the audit. Without appropriate follow up, much of the value of the audit may be lost and the credibility of the internal audit function might suffer. This process allows us to learn from reviews where our recommendations have not been implemented and understand the reasons why. Allows us to capture changes in the process and we can update our records.

- In issue tracking it is important to remember the following:
 - What to follow-up and when
 - Allow sufficient lead times

- Inputs required for issue resolution tracking:
 - Internal audit reports
 - Implementation timelines
 - Persons responsible
 - Management response on action plan status
 - Revised implementation dates

Assess Issue Resolution Activities and Compare to Action Plan

- Determine whether corrective action was taken in achieving the desired results or that senior management or the board has assumed the risk of not implementing the agreed upon corrective action.
- Determine which findings should be followed up.
- Confirm that the reported management response actually occurred.
- Evaluate the reasonableness of management response on actions.
- Assess whether the implemented action addressed the original finding.
- Collate responses and update status of actions.
- Summarise and report as appropriate

Reporting Process

- Discuss and challenge findings and observations with the audit team.
- Confirm the factual accuracy of the findings and observations with the process owner during the close-out meeting .
- Prepare a discussion draft (if appropriate) to circulate to process owner to further confirm the factual accuracy of the issues raised.

Issue Resolution and Obtaining Management Comments

- Issue a formal draft Report requesting management responses to findings and recommendations suggested—remember to version control it!
- Issue a final Report containing managements responses and their action place to address your findings and recommendations.
- Update the internal audit plan for any areas requiring further internal audit work.
- Complete audit records: files, quality questionnaires etc.

Agree issues and proposed action with Management

Success of an internal audit assigned depends on the acceptance of audit issues and proposed action by the management. The following need to be considered:

- ♦ **No findings are to be included that have not been previously discussed with auditee.**
- ♦ **Agreement needs to be reached regarding the facts of each point included in the final report. Management comments that contest audit findings reduce the credibility of the entire audit process.**
- ♦ **Management must be directly involved in the formulation of the recommendations.**
- ♦ **While developing the action plan along with the management we need to ensure that organisational objectives as well as the improvement of the control environment are taken into account.**
- ♦ **The agreed action takes the 3 Es into account, i.e., Economy, Efficiency and Effectiveness.**
- ♦ **The cost of implementing and maintaining the control is to be weighed against the possible benefits.**

Internal Audit Reporting

Steps to Report Writing

Internal auditor should ask himself :

- ◆ Why am I writing?
- ◆ Whom am I writing to?
- ◆ What kind of piece should I write?
- ◆ What action steps do I want as a result?
- ◆ What tone is right?
- ◆ What are all the points I could make?
- ◆ What points should I make, and in what order?
 - Clarify the purpose
 - Analyze the audience
 - Decide on a strategy
 - Determine the content

Report Format – Best Practice

- Introduction
- Audit Objectives
- Scope and Extent of Work:
 - agreed scope during Opening Meeting,
 - extent to indicate the sample selected and percentage vis-à-vis population of transactions,

- Executive Summary – Summarise key observations with the business implications. Put these issues in a overall perspective,
- Observations and recommendations:
 - Observations to include specific examples,
 - Root cause and Implication,
 - recommendations which are possible to implement given company constraints – this shall ensure buy-in from process owners,
 - good idea to break-up recommendations into short term and long term, and
 - management action plan – process owner and date.
- Conclusion

The report content and structure is tailored to meet the requirement of the intended audience. The report should in minimum contain the following:

- Executive summary – This is usually no more than one page with a target audience of senior executives and audit committee. The summary should focus on outlining the key issues in the report, which will allow the reader to quickly focus on the issues that require immediate attention.
- Detailed findings – detailed explanations of the audit findings, recommendations and management responses/action plans.
- An appendix - documenting the audit work performed and the people interviewed as part of the review.

Report Format – Documentation Procedure

The assessment should provide the audit teams overall evaluation of the control framework based on issues noted and management

responses. Only key issues to be discussed here which require senior management attention.

Internal Audit Reporting and Audience

Audience	Needs	Suggested Communication
Audit Committee and Senior Management	<ul style="list-style-type: none"> ♦ Focused, concise information on key needs ♦ Timely notification of critical issues ♦ Comfort that management is taking action 	<ul style="list-style-type: none"> ♦ Executive summary of the internal audit report ♦ Audit Committee Annual Report ♦ Audit Committee Periodic Report ♦ Status Report
Process Owner	<ul style="list-style-type: none"> ♦ Information to access whether the process is operating well ♦ Timely notification of significant Issues 	<ul style="list-style-type: none"> ♦ Internal Audit Report ♦ Issue Resolution tracking summary

Audience	Needs	Suggested Communication
Management within the process	<ul style="list-style-type: none"> ♦ Timely notification of process and control issues ♦ Commitment to the recommendations 	<ul style="list-style-type: none"> ♦ Summary of Issues document ♦ Internal Audit Report ♦ Issue resolution

	<ul style="list-style-type: none"> ♦ Sufficient information to implement the recommendation ♦ Action Plans 	tracking summary
External Auditor	<ul style="list-style-type: none"> ♦ Sufficient information to identify areas where the auditor can rely on our work ♦ Focused, concise information on the key issues ♦ Comfort that management is taking reasonable action 	<ul style="list-style-type: none"> ♦ Audit committee annual report ♦ Audit committee periodic report ♦ Status reports ♦ Internal Audit Report

Types of Reporting

Audit Committee Reporting

The internal audit function ultimately reports and is accountable to the organisation's Audit Committee.

Periodic Reporting

- Prepare internal audit reports for the projects performed during the audit cycle and distribute them to the members of the Audit Committee and other related parties.
- This distribution allows the committee to effectively examine and consider the issues when provided with sufficient lead time prior to the Audit Committee meeting.
- We should not overwhelm the committee with excessive details.

Training Material on Internal Audit

- Summaries are appropriate and should be supported by detail as requested by the Audit Committee.
- We should also address details of previous report follow-up and status of management's implementation of corrective actions.

Annual Reporting

- Progress against the Internal Audit plan.
- Completion against budgeted time.
- Proposed changes to the Internal audit plan.
- Issue resolution tracking.
- Performance Indicators.

Summary of individual completed projects

- Provides a concise view of the work completed to date and the associated issues and management actions, if applicable.

Sample- Internal Audit Report

A.

Sl. No.	Audit No.	Location	Function	Date of Audit	Period Covered	Obs No	Observation	Risk Level
1.		Mumbai	Cash and Bank	April 25-4th May, 2007	April 1, 2006 - March 2007	2	Person responsible for receiving cash and issuing money receipt is also responsible for transaction in the books. Some times money receipts are also not issued to the party concerned.	Med

B.

Risk Implication	Root Cause	Recommendation	Accepted (Yes/No)	Person Responsible	Implement Date
If money receipts are not issued, it may be difficult to trace physical cash receipts with amount posted to books of accounts, if the need arises at a later date.	Pre-numbered money receipts have to be generated manually at the time of receipt of cash as SAP is not customized to generate a receipt for giving the same to the payer.	It may be considered if SAP can be customized to generate money receipt as soon as cash receipt is posted, considering the conscious decision taken by the unit management to operate different activities through a single person.	Yes	XYZ.	Already implemented.

C.

Action Plan/ Reply	Latest Status
Cash receipts are being issued on a regular basis.	

Risk Matrix – X Industries Ltd (*Illustrative*)

Materials Management	Purchase and Accounts Payable	Fixed Assets	Maintenance
Statutory Compliance	Sales and Accounts Receivable	Productions and Operations	Information Technology
	Logistics and Transport	Quality Assurance	Packaging and Dispatch
	Finance and Accounts	Human Resources	Safety Health Environment

Legend

Red- High Risk
Yellow- Medium Risk
Green – Low Risk

MODULE - IV

RISK ANALYSIS and MANAGEMENT, RISK-BASED INTERNAL AUDIT

Chapter-IV.1

Introduction to Risk-based Audit and Internal Audit

The globalization of business, growing complexity of transactions and new-age IT infrastructure have revolutionized the concept of trade and commerce. However, parallel to this great upsurge, another growing factor has been haunting corporate board rooms – that is the phenomenon of ‘Risk’. This is an all pervading term covering operational, financial and regulatory domains. There can be a liquidity risk, a fraud risk, a reputational risk, a competition risk and sundry other forms of risk. To combat and reduce risk, Internal Auditors have come up with better Internal Controls. Thus the Internal Audit profession has witnessed a sea-change from the traditional typical ‘compliance’ or ‘transaction’ audit to a much more dynamic ‘Risk-based Audit’, ‘Controls Assessments’, ‘Controls Rationalization’ and so forth.

The Changing Roles and Advent of Risk-based Audit

Internal auditing is a valuable resource to executive management and the board of directors (BOD) in accomplishing overall organizational goals and objectives, and simultaneously strengthening internal control and overall governance.

In the current global scenario, internal auditing function reviews the reliability and integrity of information, compliance with policies and regulations, the safeguarding of assets, the economical and efficient use of resources, and established operational goals and objectives. Today, internal audits encompass all financial activities and operations including systems, production, engineering, marketing, and human resources. Indeed, a wide gamut of corporate activities.

Training Material on Internal Audit

The 21st century internal auditors have the following vital areas of responsibility:

- Review operations, policies, and procedures,
- Help ensure goals and objectives are met,
- Understanding of “big picture” and diverse operations, and
- Make recommendations to improve economy and efficiency.

The enhanced role of the internal auditor covers, *inter alia*,

- Risk management, control, and governance processes
- Financial analysts
- Risk evaluators
- Improving operations, business performance
- Supplying analyses, suggestions, and recommendations
- Adding Value

Some Important Services Rendered By Internal Auditors

Risk Assurance

One of the primary roles of IA is Risk Assurance. Internal auditors identify all auditable activities and relevant risk factors, and assess their significance:

- Investigating
- Evaluating
- Identifying potential trouble spots
- Communicating
- Anticipating emerging issues
- Identifying opportunities

Internal Control Assessments

Internal Audit Assesses the 'as –is' Internal Control system within the organization and map it against a globally accepted 'standard' which is basically , an Internal Controls framework- COSO being the most widely used:

- Evaluate efficiency and effectiveness of controls.
- Recommend new controls where needed – or discontinuing unnecessary controls.
- Use of control frameworks (COSO, CoCo, Cadbury).
- Control self-assessment (CSA).
- Provide on-going education and training on risks and controls.

Based on the internal audit findings, the same along with recommendations are communicated to appropriate management level for consideration and possible implementation.

- Keeping executive management aware of critical issues.
- Ensuring factual communications of financial and other data.
- Suggestions based on knowledge of operations throughout the organization.

Chapter-IV.2

Understanding Risk-based Internal Audit (RBIA) – Theory, Implications and Practical Issues

The Risk-based Internal Audit is superior to traditional audit approaches for two reasons. First, *it focuses on risks, the underlying causes of financial surprises, not just the accounting records*. Secondly, the Risk-based Internal Audit *shifts the focus from inspecting the quality of the financial information that is recorded in the financial statements to building quality into the financial reporting process and adding value to the organization's operations*.

The Risk-based Internal Audit, which focuses on both recorded and unrecorded risk, improves financial statement assurance and the financial statement reporting process. The Risk-based Internal Audit focuses on business risk and the processes for controlling these risks. The higher the risk area, the more audit time and client controls are required.

In order to identify business risks, the auditor must obtain a thorough understanding of controls, financial condition, sources of revenues, expenditures, competition and other business risks. The first goal of the Risk-based Internal Audit is to identify when an organization has failed to consider an important risk, economic event or transaction. The second goal is to assure that they have focused on emerging risks that may not yet be well understood or managed.

The Risk-based Internal Audit requires a greater understanding of the entity and more knowledge of the entity's business environment than required in a traditional one. Whenever possible, the Risk-based internal Audit approach tests and relies upon the entity's process for controlling risks that could affect the financial statements. In traditional internal audits, the auditor substantiates account balances after the fact rather than relying on a entity's

controls. This means that the auditor should evaluate the effectiveness of internal control system and place reliance on control system whenever possible.

By focusing on the client's control processes, the Risk-based Internal Audit Approach would add value to the entity by:

- addressing risks affecting the entity and their financial reporting;
- providing services that help the entity manage its business and risks;
- communicating with the entity on important issues;
- improving identification of financial statement misstatement;
- improving assessment of the entity's business viability;
- improving identification of fraud; and
- improving quality and timeliness of reporting.

Audit Methodology

Risk - Definition

A risk is defined as 'threat or possibility that an action or event will adversely or beneficially affect an organization's ability to achieve its objectives'.

Risk-based Audit (RBA)

The IIA states that Risk-based auditing 'starts with the business objectives and then focuses on those risks that have been identified by management that may hinder their achievement'. The role of the Service is to 'assess the extent to which a robust risk management approach is adopted and applied, as planned, by management across the organization to reduce risks to a level that is acceptable to the board (the risk appetite).'

Methodology

Risk Management Systems Assessment

Clearly the starting point is to undertake an assessment of the risk management process at the entity. RBIA role here is to provide training for entity staff and managers on risk management and to undertake a formal review of the entity's systems as part of the Annual Assurance Plan.

Using the entity's strategic risk register RBIA will prioritize and focus work to systematically, over the period of the strategic assurance plan to independently validate the entity's risk assessments both before, and after, controls are applied.

Independent Risk Assessment

Using independent knowledge and experience RBA will overlay risk assessment and identify significant gaps and omissions in the entity's risk assessments. This may include compliance and other significant issues relevant to the entity.

Operational, Mandatory and Compliance Work

Using a fully Risk-based methodology rightly focuses resource and assurance activity on key strategic issues. This allows RBA to add value to the entity at a macro level and to focus assurance over key strategic issues to the entity.

Using a fully Risk-based methodology does not, however, necessarily identify compliance, mandatory and operational system requirements as significant priorities for assurance. The Business Assurance Service therefore partitions resource to allocate audit resources to these areas. It is imperative to apply an operational level Risk-based assurance approach which focuses resource within reviews to key controls and mitigating actions.

Consulting Work

RBIA approach also seeks to provide collaborative, proactive support, before and during the development of processes, systems and operations at the entity.

Reporting

Reporting is designed to meet stakeholder and user requirements. Reporting aims are:

- To be within a risk assessment framework to enable comparison of reports.
- To be supported with by the audit approach.
- To provide clear conclusions and assurance.
- To clearly express priority and significance of recommendations made.

Reports primarily are, *inter alia*, intended to be:

- Collaborative
- Bespoke
- Contextual
- Designed to assist

Risk-based Internal Audit – The New Model Of The Profession

The internal audit function for organizations has had to reinvent itself in order to keep pace with the sponsoring organization, to keep pace with changing and increasingly sophisticated technology, to keep pace with the changing risk profile of organizations, and to keep pace with increasing service level expectations.

Audit methodology for internal audit has had to evolve, just as it has for the external audit profession. The old compliance method of auditing has been replaced with a more sophisticated risk-based and risk-driven planning and auditing perspective. To best

serve the sponsoring organization, the **internal audit function must first understand the business**. This understanding must include understanding the inherent risks to the business, the products, the competition, how the product is delivered and the operations.

Step 1

Create an Enterprise-Wide Risk Profile

First the entity/organization as a whole is evaluated to understand the environment of the organization, the key business risks that need to be controlled and the challenges that the organization must deal with. Other information that is assessed at this point should include the culture of the organization, the strategic plan, the current year business plan, the financial plan, and areas of known issues from prior internal audit work, as well as forthcoming changes in legislation or regulations. The enterprise-wide risk profile and control environment, as set by senior management, will drive the individual unit behaviors and priorities.

From the understanding of the corporate environment and the key risks, each business unit can be evaluated as to the degree of risk/complexity it presents. This would cover business units and support functions within an organization. Often the organization is examined following the reporting structure that the CEO has set to manage the organization. Where the evaluation of the business unit suggests high risk, further audit examination can continue looking at specific risks and in turn the controls in place to mitigate specific risks. Where a unit and its business processes are evaluated as presenting low risk to the organization as a whole, no further audit effort would be expended.

Step 2

The Business Unit

An RBIA methodology can follow a four-step process.

Step 1 - Know your client: Gain an understanding of the business unit's operations and/or corporate function and the business environment in which the unit operates.

Step 2 - Risk assessment and planning: Assess the risk profile of the business unit and plan the audit approach to address those risks.

Step 3 - Testing and evaluation: Perform the audit work in an efficient and effective manner to evaluate the results of audit tests within a business context.

Step 4 - Communicate results: Communicate audit results in the most efficient and effective manner that adds value to the auditees with an alignment to risk and business objectives.

The "know your client" phase of the audit process involves obtaining an understanding of the audit entity's operations and environment in order to assess the risks that face that business. Business risks include the economic, financial, industry and competitive risks that the unit faces and represent the primary challenges to management in achieving profitability and assuring long-term growth. As part of this process, the management control environment is assessed as to effectiveness.

In the second step of the audit process, the auditor assesses both business and audit risks. The approach taken in assessing the risk reflects a "top-down" approach whereby the general risks are assessed first, and then the more specific risks are evaluated. Similarly the evaluation of internal controls is a top-down approach in that the control environment is evaluated firstly at the senior management level, then at the manager level, and finally at the operational level. After identifying significant business risks, an evaluation of management's effectiveness in managing those risks to achieve the control objectives of safeguarding of assets and liabilities, integrity of information, compliance with laws and regulations, and also efficiency and effectiveness of operations is conducted.

After making a careful overall assessment of business and audit risks, together with an evaluation of the client's internal controls, the internal auditor then validates the evaluation by performing audit tests that are most efficient and effective in response to the risks and controls identified. The extent of audit procedures performed to validate the effectiveness of controls at process level is dependent on the auditor's evaluation of the management controls that are in place to monitor those processes.

Tools to assist the auditors in performing the work to ensure completeness and accuracy of the audit include documentation templates, process mapping, and computer data mining programs.

Effective RBIA communications

RBIA needs to follow an appropriate method of reporting the results of its work. There are two levels of assessment when providing an opinion on internal controls. The first is for RBIA to opine whether the controls as designed by management are adequate given the risk profile of the unit, the control environment of the unit, and the specific risks of the business processes. The second is whether the controls designed by management are operating effectively.

If the conclusion is that controls are not adequately designed, RBIA would need to discuss with management both the gaps that exist that allow unnecessary exposure to risk and the necessary action to resolve the deficiencies. Part of that discussion would also entail quantifying the risk that the organization is left to absorb. While this may seem extreme, it can be commonplace where internal audit is involved in auditing a proposed redesign of a process.

Assuming controls are adequately designed and audit tests can be executed, the next level of conclusion would be whether the controls as designed by management are operating effectively. This conclusion will be reached based on control breakdowns noted during the audit work and their severity given the business risk designed to be mitigated. Often RBIA uses ratings such as effective, needs improvement, or unsatisfactory. Communication of results involves rendering an opinion on the effectiveness of internal controls. Also the internal auditor should strive to make constructive comments and suggestions to improve the units' controls.

Reporting designed for senior management

While business unit management should be provided with the details of the results of the audit work conducted in the unit, the level of detail to more senior management should reflect their breadth of responsibilities. The same is true in reporting to audit committees and boards of directors. At this level they need to be

given an enterprise-wide view. At the senior levels it is important for the audit director to provide an opinion on the state of the internal controls across the organization. The board needs to be apprised if there is evidence that the control structure is weakening or if certain risks are not being adequately mitigated.

Chapter-IV.3

Risk Management and RBIA

Post Sarbanes, organizations are concerned about:

- Risk Management
- Governance
- Control
- Assurance (Consulting)

"Every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value."

Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value."

Source: Extract from COSO ERM framework

What is risk?

- A business risk is the threat that *an event or action will adversely affect an organization's ability to maximize stakeholder value and to achieve its business objectives.*
- Mathematically, *Risk is the product of probability of occurrence and the financial impact of such occurrence.*
- Risk may be broadly – *Operational, Financial and Regulatory*

Risk Types

- Credit risk
- Liquidity risk
- Market risk
- Reputation risk
- Competition risk
- Technological risk
- Regulatory risk

Risk Management is the process of *measuring or assessing risk* and *developing strategies to manage it*

Why Risk Management / RBIA

- Rate and magnitude of business change is accelerating
- Marketplace tolerance for surprises is low
- Earnings pressures continue to advance
- Benchmarks for effective governance are rising
- Compliance with regulations is a priority

Risk Definition Information

- Risk name
- Risk scope
- Risk nature
- Stakeholders
- Quantification
- Risk treatment and control mechanism
- Potential actions for improvement

Risk Management / RBIA process

1. Risk Identification
2. Risk Assessment
3. Risk Management
4. Risk plan and implementation
5. Risk reporting, review and evaluation

Risk factors

Business objectives	External risk factors	Internal risk factors
Financial performance	Macro economy	Financial reporting risks
Client and Market focus	Political environment	Liquidity
Execution excellence	Forex exchange transactions	Intellectual Property management
Organization and Development	Revenue concentration	HR management
	Technological obsolescence	Legal compliance
	Security and business continuity	Engagement execution
		Culture and values

Risk Assessment – Matrix (illustrative)

Threat Likelihood	Impact		
	<i>Low</i> (10)	<i>Medium</i> (50)	<i>High</i> (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

Risk Values (an example)

<i>Cause</i>	<i>Risk impact</i>	<i>Potential loss (Rs. Crore)</i>	<i>Probability</i>	<i>Control effective-ness</i>	<i>Resi- dual risk value (Rs. Crore)</i>
Service delivery failure	reputation	4	1.0 (High)	Strong (0.75)	1
Wrong financial plan and budget	Cost over run	3	0.5 (Medium)	0.5 (Medium)	0.75
Inadequate systems functionality	Infrastructure failure	5	0.25 (low)	Weak (0.25)	0.9375

Extracts of Risk Management reports from Annual reports (MDandA)

- **Reliance Industries Ltd. (RIL, FY 05-06)** – Risks and Concerns , Internal Control (supply, pricing inventory)
- **TCS (FY 05-06)** – Risks and Concerns and mitigation (competition, pricing, IP management)
- **Infosys (FY 05-06)** – Risk management report (skilled personnel availability, margin pressure, new technology and business models, foreign exchange transactions, talent poaching, immigration regulation changes, competition)

Enterprise Risk Management (ERM)

Enterprise risk management is ***a process***, effected by an ***entity's board of directors, management and other personnel***, applied in ***strategy setting and across the enterprise***, designed to ***identify potential events that may affect the entity***, and ***manage risk to be within its risk appetite***, to ***provide reasonable assurance regarding the achievement of entity objectives***

RBIA can add value by:

- Reviewing critical control systems and risk management processes.
- Performing an effectiveness review of management's risk assessments and the internal controls, improving operations and business performance.
- Providing advice in the design and improvement of control systems and risk mitigation strategies.
- Implementing a risk-based approach to planning and executing the internal audit process.
- Ensuring that internal auditing's resources are directed at those areas most important to the organization.
- Facilitating ERM workshops.

- Defining risk tolerances where none have been identified, based on internal auditing's experience, judgment, and consultation with management.
- Controls benchmarking

Internal Audit / RBIA Core Roles (IIA Guidelines)

- Assurance on risk management process
- Evaluating risk management process
- Evaluating key risk reporting
- Reviewing management of key risks

Internal Audit / RBIA legitimate roles with safeguards (IIA Guidelines)

- Facilitate identification and evaluation of risks
- Coaching management in responding to risks
- Coordinating ERM activities
- Developing Risk management strategies for Board approval.
- Championing establishment of ERM

Safeguards

- Management responsible for Risk Management
- Internal audit roles to be documented in audit charter and approved by Audit Committee
- IA should not manage any risk on behalf of management
- IA can advance, challenge or support management's decisions but cannot take risk management decisions themselves.

Internal Audit not to undertake (IIA Guidelines)

- Setting risk appetite
- Imposing Risk Management process
- Accepting accountability for Risk Management

Role of Internal Auditors / RBIA in Fraud Prevention

Internal auditors are responsible for helping *deter fraud* by examining and evaluating the *adequacy and the effectiveness of controls*, along with the *extent of the potential exposure and risk in the various segments* of the entity's operations.

RBIA is supposed to consider the following:

- Fostering control consciousness
- Appropriate authorization policies
- Practical and working policies, practices, procedures, reports, and other mechanisms
- MIS and communication channels

Typical Risk Factors for Project Management

- Inadequate opportunity cost analysis for projects running beyond completion time.
- Inadequate contractors due to location of project site.
- Interference of operations with project work.
- Excess transportation cost due to project location.

- Appointment of EPC contractor with inadequate skill sets and financial resources.
- Absence of price escalation clause in contracts with vendors.
- Excess time taken from approval to project initiation.
- Delay in projects which are dependant on other projects.
- Over / under estimation of time, cost and resources required for the project.
- Non payment of dues to sub-contractors / workers by contractors.
- Inadequate planning and estimation of cost during project conceptualization.
- Inadequate monitoring of expenses incurred on projects.
- Disputes with contractor.
- Excess cost incurred in completion of projects.
- Impediments in completion of expansion/ up gradation projects.
- Absence of documentation of learning's from past projects and absence of well defined corrective measures for future projects.
- Escalation in prices of raw material.
- Delay in acquiring environmental clearance.

Chapter-IV.4

Risk-based Internal Auditing Application

RBIA application provides the means to keep track of the healthiness of business, as well as following up on the necessary steps that should be taken in order to secure the business from any flaws that might weaken its performance.

Audit Universe

The cornerstone of any auditing business is defining its audit universe (i.e. its business domain) whose items will be inspected by the audit team. The audit universe is divided into 3 layers:

- Function area
- Business entity
- Sub-components

If we consider the banking environment, for instance, as a business domain, then the bank's information technology, credit and operations departments might be considered as separate functional areas within the banking business domain. In order to focus more on the business, each function area is divided into business entities. The "Business Entity" is the item that can be audited through the application. As subcomponents are related to business entities, the audit of a business entity might include all or some of its subcomponents. Audit reports and risk assessments will be generated at the business entity level while comments, resolutions and audit work programs will be related to the sub-components of the business entities.

Using the previous analogy, "Internet Banking" would be a business entity within the "Information Technology" functional area. This audit universe structure will lead to a better control over business behavior, which will lead to an overall improvement in the business.

Audit Cycle Functionalities

Planning

A fruitful audit cycle requires accurate and precise planning. Planning is the first phase in the creation of any audit cycle. It involves the following activities:

- Audit cycle definition
- Specifying auditors and their activities
- Generating the “Opening Memorandum” to all concerned parties
- Preparing the “Audit Work Program” for the created audit cycle
- Generating the “Planning Memorandum” defining all the planning activities

Fieldwork

Upon the initiation of the fieldwork, auditors will be allowed to enter the test results of their assigned processes. The test steps of each process will be accessible by only those auditors assigned to a particular process. The lead auditor of the audit cycle will be able to review the test steps and enter coaching notes, but he will not be able to modify any of the test step entries.

Closing

The activities of the closing phase will start once the fieldwork activities are completed. The main milestone of that phase is to generate the audit report to the management team. The audit report contains a list of auditing comments. A “Comment” is a serious concern – supported by at least one “Approved” finding – that needs to be taken care of. The comments are classified into 3 main categories:

- Normal comment
- Major comment
- Work-paper comment

Approval Cycle

In order to maintain control over the auditing cycles, all the important actions are subject to approval cycles. These cycles ensure that no important action is taken without being supervised by a higher authority. The following actions are controlled by approval cycles:

- Finding issuance
- Comment issuance
- Comment resolution
- Draft audit report issuance
- Final audit report issuance
- Audit cycle closure
- Resolution completeness
- Resolution due date re-targeting

Audit Cycle Transitions Monitoring

All the transition dates for an audit cycle will be kept for reporting purposes. The application will keep track of the start date and the end date of each of the audit cycle phases.

Coaching Notes

In order to enhance the auditing process and transfer the knowledge from the lead auditors to the junior ones, coaching notes and remarks are entered by the lead auditors on certain occasions.

Handling of Supporting Documents

In order to make the application the only repository that holds all the data and evidence that supports the processing of any audit cycle, the application will give users the ability to upload

supporting documents, such as; files or scanned images, on different levels. A supporting document can be attached to:

- Audit cycle (as a whole)
- Planning memo
- Test step
- Finding
- Comment
- Comment resolutions

Test Step Cross-Referencing

Users are enabled to cross-reference a test step from another test step(s). The referenced test steps will be easily accessible while navigating the contents of the main test step.

Generic Audit Work Programs

Each sub-component in the audit universe will have its own audit generic work program. The generic work program will contain the processes, risks, controls and test procedures related to a sub-component.

Risk Assessment

The risk assessment will be defined at the business entity level. It will determine the current risk level of the business entity, risks and controls associated with each of the business entity processes, the residual risk level after applying the controls and finally the composite risk level of the whole audit entity.

Audit Plans

In order to give auditors the ability to plan their work ahead, auditor management will be able to automatically generate the audit plan according to previously entered settings.

Template Creation

The main purpose of any audit cycle is to generate audit reports that are shown to the organization's senior management so they are always on track regarding the performance of their units.

All audit report templates are generated in MS-Word in order to give the user the ability to modify them according to his preference. All the data for these templates will be derived from the database so the user will not re-enter them in the templates. These templates include:

- Opening memorandum print template
- Opening memorandum e-mail template
- Planning memorandum print template
- Planning memorandum e-mail template
- Findings' template
- Audit work program template
- Risk assessment template
- Comments' template
- Work-paper comments' template
- Audit report template

Risk-based Internal Audit

Risk assessment in internal auditing identifies, measures, and prioritizes risks so that focus is placed on the auditable areas of greatest significance. In individual audits, risk assessment is used to identify the most important areas within the audit scope. Risk assessment allows the auditor to design an audit program that tests the most important controls, or to test the controls at greater depth or with more thoroughness.

Risk-based Internal auditing (RBIA) extends and improves the risk assessment model by shifting the audit vision. Instead of looking at the business process in a system of internal control, the internal

auditor views the business process in an environment of risk. It's a straightforward paradigm: an audit focusing on risk adds more value to the organization than an audit focusing only on controls.

Some customers have criticized internal auditing for being too focused on the past. "Driving the car by looking in the rear view mirror," one of the more telling metaphors, characterizes the internal auditor as one who renders advice and recommendations based on examinations of the historical transaction record and the historical operation of the internal control system.

To extend more value to clients and the organization, internal auditors must shift their focus from the past to the future. If the auditor focuses on risks, the audit is more likely to address the full range of issues that concern management.

For most auditors, the shift will be subtle. Instead of identifying and testing controls, the auditor will identify risks and test the ways management mitigates those risks. The majority of risk mitigation techniques will still involve controls; but the auditor will test "how well are these risks being managed?" rather than "are the controls over this risk adequate and effective?"

Controls themselves do not necessarily guarantee success. Major banks with hundreds of transaction controls have lost hundreds of millions by failing to understand the risk that some traders may not enter all of their commitments and transactions into the system.

Each control added to the system costs more resources to operate. If auditors continue to audit and recommend new and strengthened controls without removing any, the weight of these controls will drag the business process down.

The Value of Risk-base Internal Audit

Despite its advantages, a recent study by The IIA's Austin Chapter shows that at least one-third of all audit groups fail to use RBIA. Other less formal research seems to confirm this finding and suggests that the reasons may be:

- Risk concepts not clearly understood
- Auditors believe that risk assessment requires specialized knowledge or software.

Training Material on Internal Audit

- There is too little time for planning - the continuous "do" loop.
- Many internal audit shops feel their operation is too small to use planning tools.
- Internal auditors feel compliance/inspection/financial auditing does not fit with risk.

In fact, RBIA concepts aren't difficult, and no specialized knowledge or software is required. RBIA works for all sizes of audit groups and types of audits. Even where the audits are mandated by law, by regulation, or by a particularly opinionated boss, RBIA can help focus the scope of the audit where it is most needed. RBIA users also indicate that the reports from risk-based audits are easier to prepare and easier to "sell" without creating unnecessary friction.

RBIA sampling plans are designed to be flexible. They concentrate on the areas of greatest importance, often relying on a "stop and go" technique, allowing the sample to be expanded or curtailed, depending on error rates.

Perhaps most importantly, RBIA can also help with the "value crisis" that appears to be affecting the audit profession, since the audits meet the needs of clients. As a result of their risk-focused approach, Royal Bank, whose story appears below, has experienced shorter audits and more effective audit reports that communicate in the language of recipients.

Putting the Paradigm to Work

The COSO model dictates a sequence of events for the management of business processes in a control environment:

1. Establish Organization Objectives
2. Assess Risk
3. Determine Controls Required

For example, in a typical purchasing audit, the internal auditor may assess and prioritize the risks to achieving the organization's purchasing objectives, which are "To provide the right goods and

services at the right price, in the right quantities, with the right quality, in the right locations, at the right time, and from the right vendors." In this instance, the auditor considers the risks to achieving these goals and determines what controls, if any, are in place to mitigate these risks. The audit process tests the controls to determine their adequacy and effectiveness. The internal auditor reports the results of these tests: "We performed an audit of the adequacy and effectiveness of the internal control system over purchasing. We found ..." The audit likely results in findings and recommendations for new or improved controls.

In an environment of risk, managers must be concerned with more than just internal control. To avoid all or some risk, managers may choose to diversify and to enter into agreements to share the consequences of risk through contracts, warranties, guarantees, and insurance. Managers may even decide to accept some risks. In many cases, these strategies may be more cost-effective means of managing the risk in the business process than applying additional controls.

Risk-base Internal Audit and the New Paradigm

Risk-based internal auditing using a new paradigm means broadening the perspective of internal auditing to include all risk management techniques, including management techniques other than control activities. This practice also gives the auditor an opportunity to examine the business process for excessive control - allowing the auditor the rare opportunity to recommend fewer controls as outdated and inefficient methods are identified.

According to The IIA's Statement of Responsibilities of Internal Auditing, the purpose of internal auditing is to examine and evaluate the organization's activities and to furnish analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed. Each audit has an audit objective, and that objective is related to furnishing the results of the examination and evaluation of activities.

Each audit is designed to accomplish the audit objective through one or more audit tests, which provide the evidence used by the

Training Material on Internal Audit

auditor to draw a conclusion and form an opinion. The sum of the conclusions and opinions is the audit result. There is a logical progression from the entity's purpose or mission to the audit performed. During the audit planning stage, the internal auditor should ensure that:

- There is a positive link between the audit objective, the goals of the auditable unit, and the entity's purpose and mission.
- The audit program, taken as a whole, will produce the evidence required to accomplish the audit objective.
- Each test will provide the evidence required in the audit program.

The audit objective should be related to the risks faced by the auditable unit in its effort to meet its established objectives. Audit tests are then linked to support the audit objective.

In the previously cited purchasing audit example, the internal auditor performed a risk assessment and then audited the controls. RBIA uses the same purchasing process goals and objectives and the same risk assessment as the traditional audit, but the next steps are very different.

In the RBIA version of the audit, the internal auditor considers the same risks to achieving the goals established by the purchasing department and determines what management is doing, if anything, to mitigate these risks. The audit consists of tests of these mitigation activities - including, but not limited to internal controls - to determine their adequacy and effectiveness.

The internal auditor reports the results of these tests in a slightly different form: "We performed an audit of the adequacy and effectiveness of management's response to the business risks in the purchasing process. We found ..." The audit likely results in an assessment of the state of risk mitigation given the current state of risk.

In other words, **RBIA starts and ends with the consideration of business risks**. Internal control is a major part of risk mitigation, but it is not the entire solution. Internal auditors will be more likely to note and recommend the appropriate level of controls and other means of mitigating the risk, even if it means pointing out that some controls are no longer appropriately scaled to their risks.

In the new paradigm, the various parts of the audit process are linked to the goals and objectives through the risk to achieving those objectives and the strategies management has adopted to mitigate that risk. The old paradigm tries to get to the same conclusion by examining how the system is controlled, which is only one of three ways that the risk can be mitigated. RBIA contributes to management's efforts to keep the business process lean and responsive over time by avoiding the layering effect of traditional controls-focused auditing.

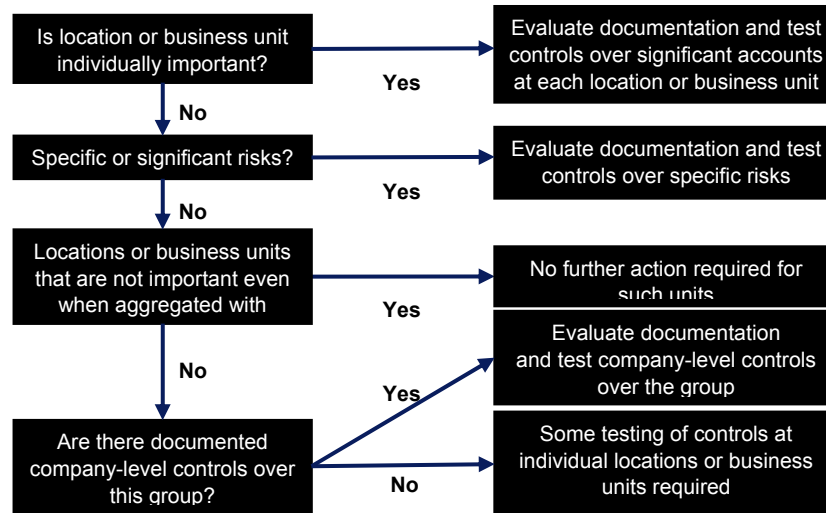
The Basics

Risk-based internal auditing should be within the abilities of all internal auditors. The processes involved in using the new paradigm are much the same as those in traditional auditing:

- List **the process** steps, tasks, or components of the system.
- Rank the steps in order of their **criticality** in achieving the unit's goals and objectives. A collaborative approach is recommended for this step. The process owner is likely to have a better understanding of the importance of various sub-units.
- Answer the following questions about each step:
 - What is the risk? What could go wrong?
 - What are the risk management activities, including controls that mitigate risk? (There may be several entries for each step, task, or component.)
 - What is the best evidence that these mitigation techniques are working as intended?
 - What test produces that evidence?

Chapter-IV.5

Planning and Scoping Multi-location RBA Engagements – Important Considerations



Step 1: Location or business units individually significant

- Level of financial significance that could result in material misstatement
- Management and the auditor must obtain evidence of design and operating effectiveness at all individually important locations
- Management and the auditor should obtain a large portion of coverage of operations and financial position

Step 2: Specific or Significant risk.

- Accounting and reporting complexities

Step 3: Locations considered important when aggregated with others

- Evaluate/test company-level controls, if applicable, or perform detailed evaluation and tests of controls over significant accounts and disclosures at that location
- This portion = 20% to 25% of consolidated operations and financial condition

Step 4: No work at locations or business units which in the aggregate could not be material

- This portion would represent less than 5% of consolidated operations and financial condition

Critical issues –

- Validate location coverage with your external auditors
- Management in all locations need to be “on-board”
- Monitor locations that are growing
- Do not underestimate “Limited Scope” locations
- Re-assess significant locations every quarter
- Assess potential acquisitions
- Be aware of language considerations
- Lack of understanding of control-based approach and proposed standard
- Documentation and testing around “softer” side of COSO
- Services Organizations in foreign countries
- Significant coordination effort
- Potential shortage of GAAP competencies

Chapter-IV.6

Risk Reporting

Draft German Standard No. 5 (*Relevant Excerpts only*)

*The principles are set out in **bold type**. They are explained in the following paragraphs which are printed in standard type. The principle of materiality is to be observed in applying the Standard.*

Scope

1. This Standard should be applied in reporting risks affecting the future developments of a group in its management report.

2. Risk reporting should provide the users of the group management report with information which is both relevant for decision-making and reliable. This information should allow users to form an appropriate picture of the risks affecting the future developments of the group.

3. This Standard applies to all parent enterprises which are required to report on the risks affecting the future developments of a group:

.....

.....

.....

Definitions

9. The following terms are used in this Standard with the meanings specified:

A *risk* is the possibility of a future negative impact on the economic position of a group.

An *opportunity* is the possibility of a future positive impact on the economic position of a group.

***Risk categories* combine risks which are similar and related to each other from an organizational or functional point of view.**

***Risk management* is a comprehensive set of control procedures covering all activities of an enterprise; these procedures are based on a defined risk strategy applying a systematic and consistent approach with the following components: identification, analysis, measurement, control, documentation and communication as well as the monitoring of these activities.**

Risk management must be an integral component of the business, planning and control processes. It should be linked with other management systems and be supported in particular by the following functions: business planning, controlling and internal audit.

Procedures

- 10. The contents and scope of the report should depend on the specific circumstances of the group and its enterprises as well as on the market and industry specific environment.**
- 11. The information provided in the risk report should focus first and foremost on the specific circumstances of the group and on the risks affecting its business activities.**
- 12. A risk which threatens the existence of the group should be clearly described as such.**
- 13. Information should be provided in particular about concentrations of risk.**
- 14. Examples are: dependence on individual customers, suppliers, products or patents.**
- 15. Individual risks should be classified in a suitable manner into risk categories.**

16. This should be based on the risk categorization used internally for the purposes of risk management.

17. The information provided on risks should be self-contained. Individual risks and the possible consequences of such risks should be described.

18. The way in which risks are presented should reflect their significance to the group. It may be helpful to evaluate the probability of occurrence of the risks and to quantify their possible effect.

19. Risks should be quantified where this can be done with reliable and recognized methods, where it is economically justifiable and where quantification could affect the decisions of the users of the group management report. In this case, the models and assumptions used should be described.

20. The requirement for risks to be quantified applies effectively therefore only to financial risks.

21. Where it is important for the assessment of individual risks, the risk should be described before taking into account the effect of any risk reduction measures to mitigate risk. A description of the measures should also be provided.

22. If a specific risk can be mitigated reliably by a particular action e. g. by entering into a contract or taking up insurance coverage, it is only necessary to report the residual risk. If this is not the case, the risks should be disclosed before taking into account the effect of any risk reduction measures to mitigate risk and the measures themselves should also be described. Where, for example, risks are covered by write-downs or provisions recognized in the financial statements, disclosures are only required to be made if this is significant for the overall assessment of the risk position of the group.

23. Risk assessment should be based on an appropriate forecast period for each risk.

24. In the case of risks threatening the existence of an enterprise, the forecast period should be at least one year. The

assessment of other significant risks should generally be based on a period of two years. In the case of enterprises with longer market cycles or where enterprises are involved in major projects, it is recommended that a longer risk assessment period is used.

25. It is preferable that inter-dependencies between individual risks are described; it is mandatory to do so, where an appropriate assessment of the risks is otherwise not possible.

26. Risks may not be set off against opportunities.

27. In order to allow a better assessment of risks, enterprises may also provide information about opportunities. This should not, however, lead to a distortion of the position of the group such that users of the financial report are no longer able to assess the risks.

28. Risk management should be described in an appropriate manner.

29. The risk management system should be presented in such a way as to enable users of the financial report to reach a better understanding of the risks affecting the group. The strategy, procedures and organization of the risk management should be described.

30. For the sake of clarity, information about risks should be presented in a self-contained section of the group management report. References to other parts of the financial statements or to other sections of the group management report may be appropriate if this does not impair the transparency of the information.

31. Information about risks should be disclosed separately from disclosures relating to anticipated developments

33. Risk reporting should be based on the position of the group at the time when the group management report is authorized for issue.

34. Significant changes compared with the previous year should be disclosed where this is necessary for an assessment of the risks.

Appendix A

Example showing categorization of risks

The following example shows how risks could be categorised for the purpose of risk reporting:

I. Business environment and industry risks

- political and legal developments.
- environmental catastrophes / war.
- risks relating to the economy.
- actions of competitors.
- market risks (volume/ price risks).
- industry and product development.

II. Strategic business risks

- product range.
- investments in other enterprises.
- capital expenditure.
- location.
- information management.

III. Performance risks

- development.
- manufacturing.
- purchasing.
- sales.
- logistics.

- environmental policy.

IV. Personnel risks

- employee recruitment.
- personnel development.
- fluctuation.
- key persons.

V. Information technology risks

- data security.
- availability (risk of breakdown/ data loss).

VI. Financial risks

- liquidity.
- currency exchange rates.
- interest rates.
- market prices of securities.
- default risk.

VII. Other risks

- organisational and management risks.
- legal risks.
- tax risks / tax field audits.
- health and safety risks.
- management and control systems.

Chapter-IV.7

Risk Evaluation Form (Illustrative)

Date: _____

Division: _____

Department: _____

Business Function: _____

PURPOSE OF THE RISK EVALUATION

The purpose of the risk evaluation is to identify the inherent risk of performing various business functions. Audit resources will be allocated to the functions with the highest risk. The risk evaluation will directly affect the nature, timing and extent of audit resources allocated.

The two primary questions to consider when evaluating the risk inherent in a business function are:

- What is the probability that things can go wrong? (the **probability** of one event)
- What is the cost if what can go wrong does go wrong? (the **exposure** of one event) Risk is evaluated by answering the above questions for various risk factors and assessing the probability of failure and the impact of exposure for each risk factor. **Risk** is the probability times the exposure.

The risk factors inherent in business include the following:

- | | |
|-----------------------|---|
| * access risk | * business disruption risk |
| * credit risk | * customer service risk |
| * data integrity risk | * financial/external report misstatement risk |
| * float risk | * fraud risk |

Risk Evaluation – It Audit (Illustrative)

- * legal and regulatory risk * physical harm risk

These risk factors cause potential exposures. The potential exposures include (but are not limited to):

- * financial loss
- * legal and regulatory violations/censorship
- * negative customer impact
- * loss of business opportunities
- * public embarrassment
- * inefficiencies in the business process

The evaluation should **NOT** consider the effectiveness of the current internal control environment. The evaluation should focus on the risks and exposures inherent to the function being evaluated. However, while performing the risk evaluation, the auditor should consider what controls are needed in order to minimize, if not eliminate, the risks and exposures.

DEFINITION OF SCOPE OF THE BUSINESS FUNCTION UNDER EVALUATION

Provide a definition of the scope of the risk evaluation.

BUSINESS FUNCTION / BUSINESS REASON

Provide a high level overview of the area, function, or application being evaluated.

ACCESS RISK	Probability	Exposure
Access risk refers to the impact of unauthorized access to any company assets, such as customer information, passwords, computer hardware and software, confidential financial information, legal information, cash, checks, and other physical assets. When evaluating access risk the nature and relative value of the company's assets need to be considered.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

BUSINESS DISRUPTION RISK	Probability	Exposure
Business disruption risk considers the impact if the function or activity was rendered inoperative due to a system failure, or a disaster situation. Consideration is given to the impact on Company customers as well as other Company operations.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

CREDIT RISK	Probability	Exposure
Credit risk considers the potential that extensions of credit to customers may not be repaid. There is an element of credit risk in each extension of credit. When setting lending policies and procedures, the company must consider what level of credit risk is acceptable. Extension of credit includes the use of debit cards and credit cards by customers to make EFT purchases.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

CUSTOMER SERVICE RISK	Probability	Exposure
Customer service risk considers the likely impact on customers if a control should fail. A customer may be external or internal to the company. For example, the line units are customers of the support units. When the customer is internal, assessment of customer service risk should also consider how problems with internal services will likely impact the level of service offered to the outside customer.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

DATA INTEGRITY RISK	Probability	Exposure
<p>Data integrity risk addresses the impact if inaccurate data is used to make inappropriate business or management decisions. This risk also addresses the impact if customer information such as account balances or transaction histories were incorrect, or if inaccurate data is used in payment to/from external entities. The release of inaccurate data outside the Company to customers, regulators, shareholders, the public, etc. could lead to a loss of business, possible legal action or public embarrassment.</p>	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

FINANCIAL/EXTERNAL REPORT MISSTATEMENT RISK	Probability	Exposure
<p>Financial/external report misstatement risk is similar to data integrity risk. However, this risk focuses specifically on the company's general ledger and the various external financial reports which are created from the G/L. Consideration of Generally Accepted Accounting Principles and regulatory accounting principles is an important factor in evaluating financial report misstatement. This risk includes the potential impact of negative comments on the external auditor's Notes to Financial Statements or Management Letter.</p>	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

FLOAT RISK	Probability	Exposure
<p>Float risk considers the opportunity cost (lost revenues) if funds are not processed or invested in a timely manner. This risk also addresses the cost (additional expenses) if obligations are not met on a timely basis. Receivables, Payables and suspense accounts are subject to float risk.</p>	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

[illegible]

FRAUD RISK	Probability	Exposure
Both internal and external fraud risks need to be considered. Internally, employees may misappropriate company assets, or manipulate or destroy company records. Externally, customers and non-customers may perpetrate a fraud by tapping into communication lines, obtaining confidential company information, misdirecting inventories or assets, etc.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

[illegible]

LEGAL AND REGULATORY RISK	Probability	Exposure
<p>In evaluating legal and regulatory risk, consider whether the product, service, or function is subject to legal and regulatory requirements. regulatory requirements may be federal, state or local. The relative risk level of an objective may be high if the related law/regulation is currently on the most dangerous violation list. Legal risk also considers the likelihood of the company being sued under a civil action for breach of contract, negligence, misrepresentation, product liability, unsafe premises, etc.</p>	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

PHYSICAL HARM RISK	Probability	Exposure
Physical harm risk considers the risk of harm to both employees and customers while in the Company premises or while performing company business. This risk also applies to company assets such as computers or other equipment which may be damaged due to misuse or improper set-up and storage, or negotiable instruments and other documents which may be damaged or destroyed.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

OTHER CONSIDERATIONS	Probability	Exposure
Consider the impact of all other relevant factors on risk. Consider, for instance, the transaction volumes (items and dollars), and financial impact on the balance sheet and income statement.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Rationale

OVERALL RATING	Probability	Exposure	Overall Risk
Based on the evaluation of: What can go wrong ? (probability); and what is the cost if what can go wrong, does go wrong ? (the exposure); evaluate the overall magnitude of the risk in the area/function. Evaluate the Probability and Exposure, then combine the two for an estimate of Overall Risk of business mission failure.	<input type="checkbox"/> High	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low	<input type="checkbox"/> Low

Rationale

AUDIT APPROVALS

Prepared by: _____ Date: _____

Approved by: _____ Date: _____

CLIENT APPROVAL

Approved by: _____ Date: _____

Chapter-IV.8

RBA/ RBIA Templates, Flowcharts, Formats and Registers (illustrative list)

A. Risk Categorization Matrix (illustrative)

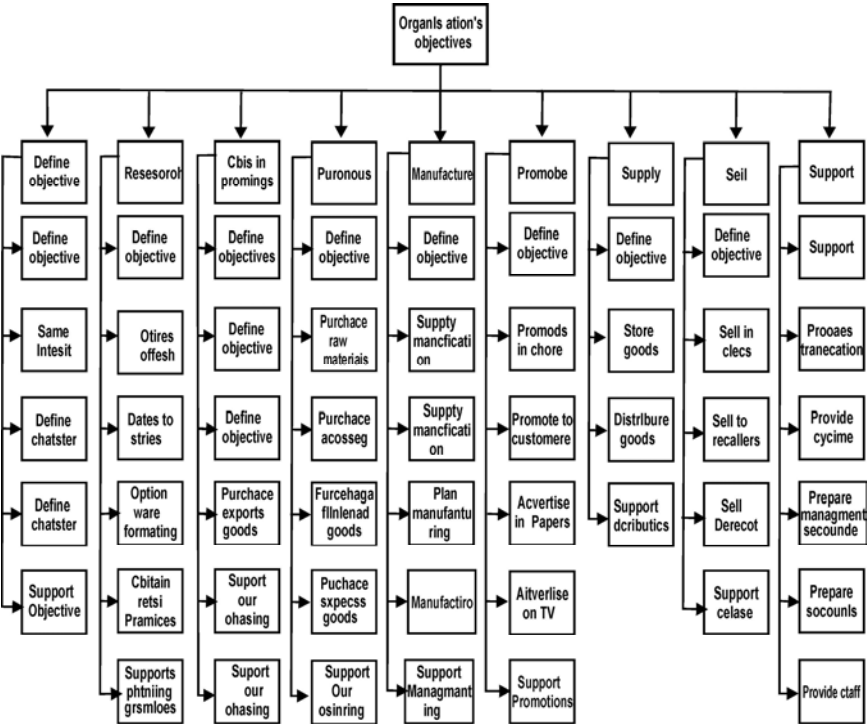
If the consequence when the risk occurs is:	the likelihood of the risk occurring is:	Then the measure is defined to be:
Acatastrophic impact on the organisation, threatening its existence Cash at risk > £1,000,000	Almost certain	Catatrophic (5)
To prevent the organisation achieving all, or a major part, of its objectives for a long time. Cash at risk < £1,000,000 > £100,000	Probable	Major (4)
To stop the organisation achieving its objectives for a limited period. Cash at risk < £100,000 > £30,000	Possible	Moderate (3)
To stop the organisation achieving its objectives for a limited period. Cash at risk <£30,000 > £5,000	Unlikely	Minor (2)
To cause minor inconvenience, not affecting the achievement of objectives Cash at risk < £5,000.	Rare	Insignificant (1)

B. Risk Readiness Matrix (Illustrative)

	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	Audit test (core IA roles in brackets)
Key characteristics	NO. formal approach developed for risk management	Scattered silo based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined	Enterprise approach to risk management developed and communicated	Risk management and internal control fully embedded into the operations	
Process						
Are the organisation's objectives defined ?	No	In Part	Yes			Check the organisation's objectives are and determined by the board and have been have been communicated to all staff. Check other objectives and target are consistent with the organisation's objective. (1)
Have management have been trained to understand what risks are and their responsibility for them?						Interview managers to confirm their understanding of risk and the extent to which they manage it. (1)
Has a scoring system for assessing risks been defined ?						Check the scoring system has been approved communicated and is used. (2)
Have process been defined to determine risks, and these have been followed?						Examine the processes to ensure the are sufficient to ensure identification of all risks. Check they are in use, by examining the output from any workshops. (1)
Have all risks been collected into one list? Have risks been allocated to specific job titles?						Examine the Risk Universe. Ensure it is complete, regularly reviewed, assessed and used to manage risks. Risk are allocated to managers. (1)

	Risk native	Risk aware	Risk defined	Risk managed	Risk enabled	Audit test (core IA roles in brackets)
Do management provide assurance on the effectiveness of their risk management?	No			In Part	Yes	Examine the assurance Provided, for key, check that controls and the management system of monitoring, are operating. (4)
Are managers assessed on their risk management performance?						Examine a sample of appraisals for evidence that risks management was properly assessed for performance (1)
Internal Audit approach	Promote risk management and rely on audit risk assessment	Promote enterprise-wide approach to risk management and rely on audit risk assessment	Facilitate risk management/liaise with risk management and use management assessment of risk where appropriate	Audit risk Management Processes and use management assessment of risk as appropriate	Audit risk Management Processes and use and use management of risk risk as appropriate	

C. Process Map



D. Risk and Audit Universe (illustrative)

Key risk to process	Response	Control (examples)	Monitoring (examples)	Cous	Like	Score	Control score	Audit action	Next audit number	Next audit name	Next timing
the objective will not deliver the organisation's objectives effectively and effectively	treat	Overall targets for sales and profits are set by the board in the budget package the Merchandise Director outlines the action to be taken to achieve the targets see case strategy controls	Monthly reports of sales and Profits are presented to the Board, with an explanation of variances	5	1	5	20	audit	200	selling strategy	jun-06
Fai to stok90005 which the customers went to buy	treat	Regular visits by Merchandising Director and staff to markets which anticipate at trade shows, focus Groups	Quarterly Presentation to Board by Merchandising Director on Market trends	5	1	5	20	audit	2001	Market anticipation	jun-06
Fai to anticipate the competitors' intentions to take a bigger market share	treat	All competitors' advertising campaigns monitored with a weekly report to the Merchandising Director	None	5	1	15	20	audit	2001	Market anticipation	jun-06
Prices are not Competitive	treat	Competitors' prices are monitored every week, with Report going to appropriate Reading of Merchandise Department	None	5	1	10	15	consultancy	2001	Market	Feb-06
Store layout confuses customers	treat		None	5	1	16	15	consultancy	203	Store Planning	Mer-06
Prices are incorrect	treat	Retail prices are input by an assistant buyer and by an assistant buyer and checked by a supervisor prices are downloaded onto the EPOS system overnight	A gross profit exception report is generated for any changes to Gp >5% This should pick up any incorrect input of retail Prices the reports is signed off by a buyer.	4	1	4	16	audit	204	Price file maintenance	Apr-06

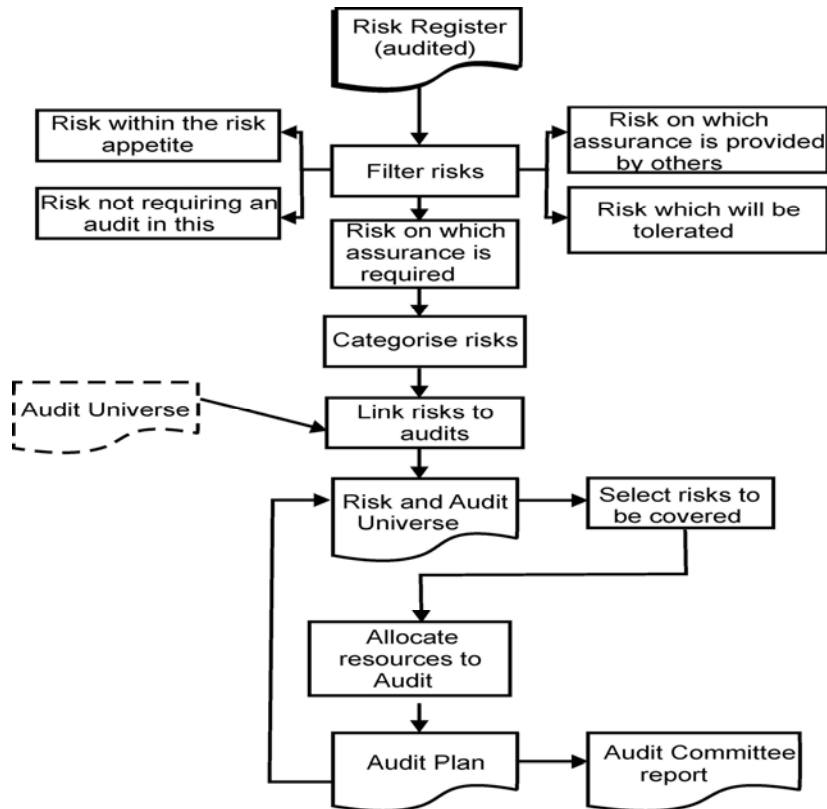
E. Audit Conclusions (illustrative)

Conclusion on:	Criteria		
Risk have been identified, evaluated and managed	Thorough processes have been used and all significant risk should have been identified	Processes have been used, but there are some deficiencies and not been identified.	Inadequate, or no, processes have been used.
Internal controls reduce risks to acceptable levels (that is to within the risk appetite of the organisation)	Risk are being managed to within acceptable levels, as defined by the board Report as Supplementary issue, if cost effective controls can reduce the risk further, otherwise do not report	Not all risk are being managed to within acceptable levels as defined by the board, although the consequence from the risk occurring, or likelihood of the risk occurring, is not considered significant there is the possibility that some objective will not be achieved Report as: Key issue	this risk is not being mitigated to an acceptable level by the control (s) and it is probable that some objective will not be achieved, with significant results Report as: Key issue No action is being taken
Action being taken to promptly remedy significant failings or weaknesses	the action being taken will result in all risks being managed to within acceptable levels	the action being taken will result in some reduction in risk but not to acceptable levels	OR insufficient action is being taken to manage risks to within acceptable levels
current levels of monitoring are	no more monitoring is necessary	Some additional monitoring is required	Major improvements are required to the monitoring of controls
Colour:	Green		
Grading:	Acceptable	Issues	Unacceptable

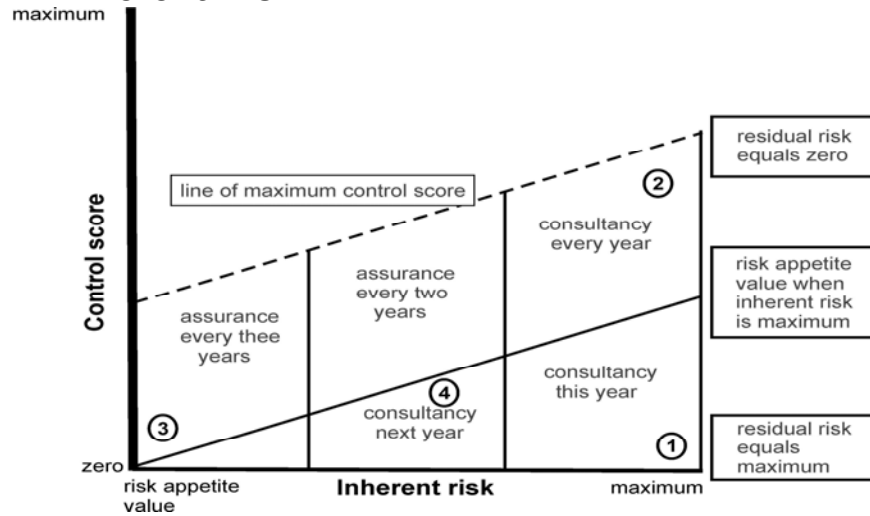
F. Risk, Controls and associated Audit approach

	Controls	Monitoring	Audit approach
Risk enabled	All risks identified and assessed. Regular reviews of risks. Responses are in place to manage risks	Management monitor that all types of response are operating properly. All managers provide assurance on the effectiveness of their risk management and are assessed on their risk management performance	Assurance
Risk managed		Management monitor that all types of response are operating properly. Most managers provide assurance on the effectiveness of their risk management and are assessed on their risk management performance	
Risk defined	Majority of risks identified and assessed. Regular reviews of risks. Responses are in place to manage most risks	Some management monitoring that all types of response are operating properly	Consultancy
Risk aware	Controls may be in place but are not linked to risks	Little monitoring	
Risk naive	Controls, but some may be missing or incomplete	Very little, if any monitoring	

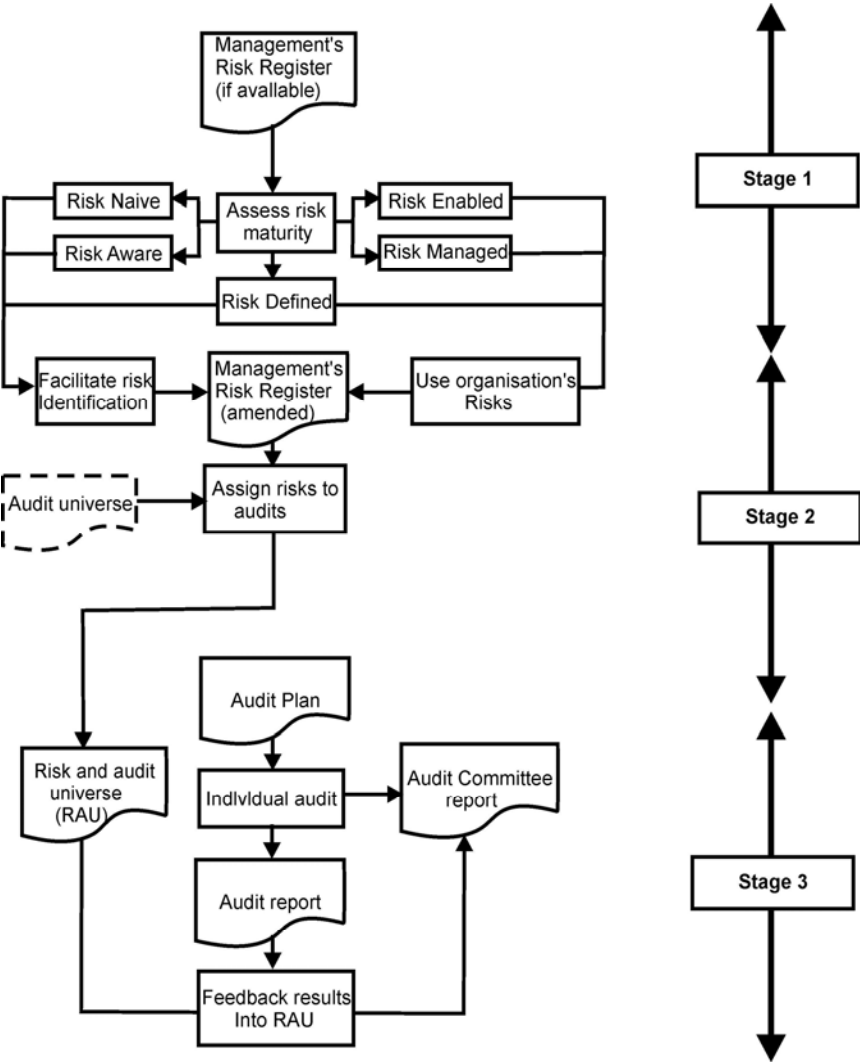
G. Risk Assessment Process



H. Inherent Risk



I. RBA Stages



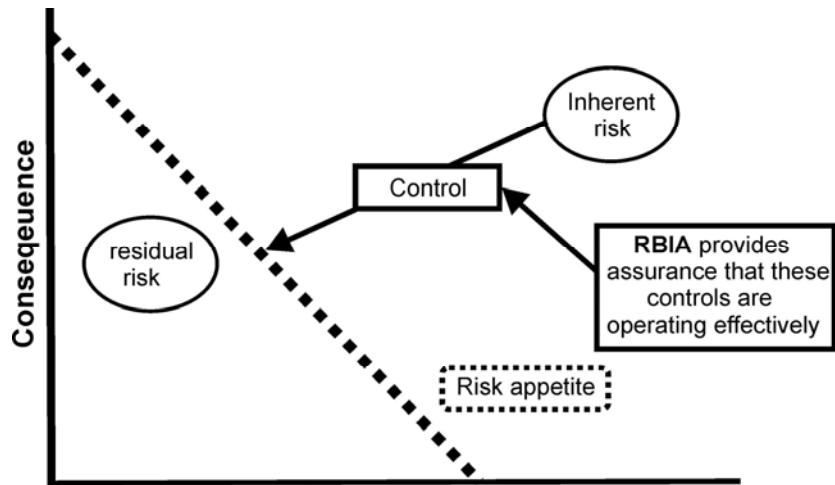
J. Risk scoring matrix

Likelihood of risk Rare(1) Unlikely (2) Possible (3) Probable (4) Almost certain (5)	5 Supplementary Issue	10 Issue	10 Unacceptable	20 Unacceptable	25 Unacceptable
	4 Acceptable	8 Supplementary Issue	12 Issue	15 Unacceptable	20 Unacceptable
	3 Acceptable	4 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue
Insignificant (1) Minor (2) Moderate (3) Major (4) Catastrophic(5)					
Consequence of risk					

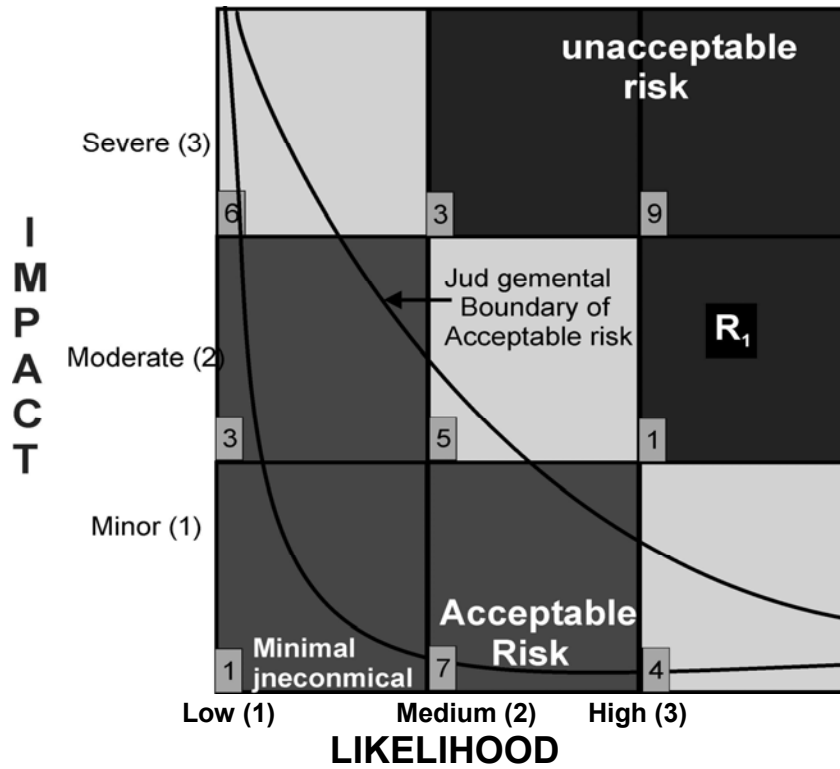
Unacceptable : Immediate action required manage the risk
Issue: Action required to manage the risk
Supplementary issue: Action is advisable if resources are available
Acceptable: No action required
 ■ ■ ■ ■ Risk appetite, as defined by the board

IR=Inherent Risk RR = Residual Risk

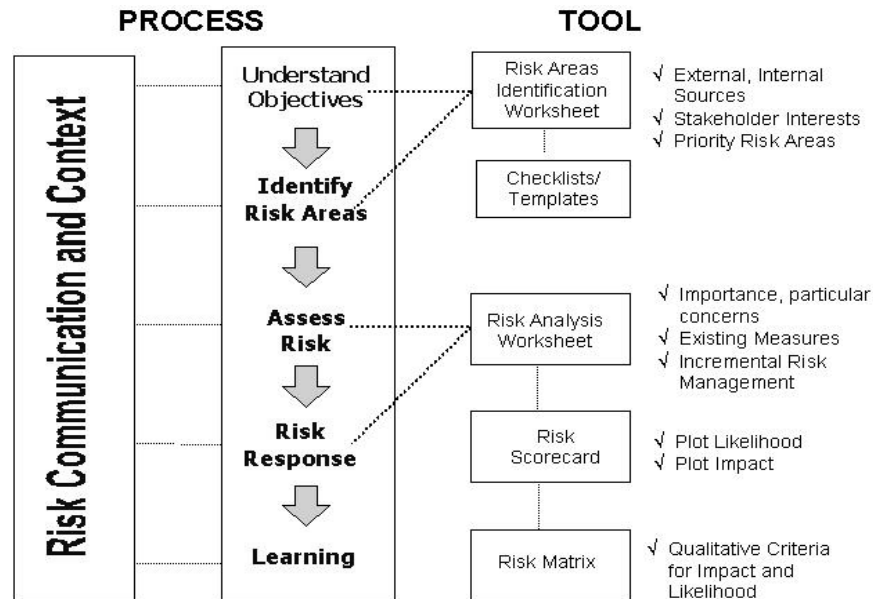
K. RBIA Objectives



L. Risk – likelihood Impact matrix



M. Risk Communication



N. Risk Management Actions Template

Impact	Risk Management Actions		
Significant	Considerable management required	Must manage and monitor risks	Extensive management essential
Moderate	Risk may be worth accepting with monitoring	Management effort worthwhile	management effort required
Minor	Accept risk	Accept, but monitor risk	manage and monitor risks
	Low	Medium Likelihood	High

Chapter-IV.9

RBIA in Banks

Risk-based Audit in a Commercial Bank

With increase in delegation of greater autonomy in financial operations, increase in volume of cross border business, greater international financial linkages, wider range of products and services and the growing diversities and complexities of banking business have increased the risks faced by banks. Risk management and risk mitigation techniques have therefore acquired paramount importance in banking business.

The banking regulators and the Bank management need an assurance in risk management compliance. Modern Risk-based internal audit must add value in the current competitive banking environment and the increasing expectations of regulators, governments and professional bodies reflect the growing importance placed on the function.

The **Basel Committee** on Banking Supervision's Internal Audit Principles, is one of the most significant developments to affect bank internal audit in recent years. And when we add to this the implications of Basel II Capital Accord and the requirements for the formal management of operational and other types of risk, the various challenges facing the banking sector become obvious.

Key Issues

The key issues are:

- Understanding the implications of the **latest developments in internal audit** for the bank and the various influences and pressures on the function.
- Authoritative guidance on the **Basel Committee's Best Practice Principles** for internal audit.
- Up-date on the very **latest professional internal audit standards** and what they mean in practice.

- How to develop internal audit service in line with **international best practice**.
- Techniques of **risk profiling** of business locations, products and activities – techniques of risk rating of branches and compilation of risk matrix.
- **Analysis of risk profile** to target audit work.
- **Modalities for conducting of Risk-based internal audit** and documentation of Risk-based internal audit reports.
- Confidence in using cost-effective techniques to evaluate bank's internal control systems in accordance with both local demands and international models such as **COSO Integrated Control Framework** and **Basel requirements**.
- Understanding the current and **future requirements for risk management**, corporate governance, management control and Risk-based auditing, and being in a position to assess the organization's current level of compliance.
- Ability to **apply the essential principles and practices** of modern audit.
- Techniques in managing, planning, performing and reporting on a wide range of audit assignments.
- Knowledge of latest corporate governance and risk management developments, including the **COSO Framework for Enterprise Risk Management**.

The Target Group

- Senior staff of bank's internal inspection department, responsible for switchover from transaction based audit to Risk-based audit and establishing, directing or developing internal audit functions within banks.

Audit managers charged with improving the audit service, leading audit teams, supervising assignments and reporting results.

Training Material on Internal Audit

- Audit staff responsible for performing audit work in accordance with in-house standards, regulatory requirements and international best practice.
- Senior staff of bank's information technology departments responsible for strengthening the IT function to meet the upcoming challenges.
- External auditors, regulators, central bank officials and others with a duty to evaluate the quality of banks' internal audit functions and enhance their utility.
- Members of bank audit committees.
- Members of faculty at national level and bank level training institutes/colleges.

Key topics and focus areas for RBIA (An indicative List)

- Nature of modern internal audit, developing role of audit: from an inspection to a consulting role
- Forms of auditing
- Objectives, responsibilities, scope and contribution of modern internal audit
- Auditing standards and other guidance
- Concept of value-added internal audit
- Developments in other countries and regulators views
- Challenges and opportunities for internal audit
- Corporate Governance, control assurance and risk management
- Implications for internal audit
- Basel Committee on Banking Supervision: Best Practices in internal audit

- Changing role of internal auditor
- Best Practices in Internal Audit
- Institute of Internal Auditors (IIA) Professional Practices Framework
- Understanding and implementing the revised IIA standards and other guidance
- Practical aspects
- Risk Identification and Risk Control:
 - Credit Risk
 - Market Risk
 - Operational Risk
 - Other Risks
- Role of Internal Audit in risk identification and risk control
- Identification, measurement and mitigation of various risks faced by a commercial bank
- Risk Assessment of various commercial banking functions
- Review and evaluation of risk management and risk control process
- What are internal controls and what should they achieve
- Internal control limitations
- Control assurance: who provides the assurance and how
- Understanding COSO, COCO, COBIT, Turnbull guidance and other important internal control frameworks
- Use of control frameworks in practice
- Relation between internal audit and internal control

Training Material on Internal Audit

- Background to and nature of guidance
- Generally observed internal control weaknesses
- Basel Committee on Banking Supervision: Understanding 13 principles of internal control framework in banks
- Management oversight and control culture
- Risk recognition and assessment
- Control activities and segregation of duties
- Information and communication
- Monitoring activities and correcting deficiencies
- Evaluation of control systems by supervisory authorities
- Implementation : practical aspects
- What is Risk-based audit
- Why switch-over to Risk-based internal audit
- Basic principles and elements of Risk-based audit framework
- Objectives of Risk-based internal audit
- Scope and functions of Risk-based internal audit
- Design of Risk-based audit
- Policy for Risk-based audit
- Risk profiling of auditees units and classification into various risk categories
- Compilation of risk matrix for audit planning
- Conduct of Risk-based internal audit—the auditing process
- Formulation of Risk-based audit plan
- Design and development of audit report formats and templates
- Deployment of internal audit resources.

- Risk-based audit planning and understanding the system
- Assessing the controls and other risk mitigation techniques
- Testing controls and performance
- Evaluating findings and reporting
- Risk-based audit planning
- Resource and other implications of audit plans
- Auditor's authority, competence and confidence
- Design of Risk-based internal audit report formats
- Auditing risk management
- Reliability of MIS and management and financial reporting
- Evaluation of policies and procedures for discharge of responsibilities
- Bank's compliance with Government laws, rules and regulations
- Adequacy of control over assets, liabilities, claims and contingencies
- Risk in communication and publication—quality control
- Auditing other strategic functions, risks and processes
- How to perform effective branch audit
- Audit risk concept comprising control risk, inherent risk and detection risk
- Identification of audit risk—risk in audit strategy, audit planning and audit process
- Maintenance of working papers
- Audit process review and quality assurance report
- Audit performance evaluation

Training Material on Internal Audit

- Recording of Audit findings-formulation of recommendations –management response-- implementation of suggestion
- Concept of control self assessment
- Levels of control self assessment
- Comparison of traditional internal audit and control self assessment
- Approaches to control self assessment
- Enhancement of information technology for risk management and risk control
- Aligning IT functions in line with regulatory requirements, business requirements and customer requirements
- Strengthening information systems, data warehousing and data mining for Risk-based internal audit requirements
- Concept of information systems
- Need for information systems audit
- Information technology for risk management
- Best practices in information technology
- Organizational, administrative, procedural control and data processing
- Adequacy of physical security measures for computer systems and records
- Accuracy and validity of the information/data processed by computer systems
- Communication with Bank Management
- Liaison and communication with External Auditors, other Banks, International organizations
- The above contents are indicative only.

Chapter-IV.10

RBIA Questionnaire (Illustrative only)

S No	Question	Management Response
1	Does the internal audit function enhance corporate governance in terms of strategy and planning, enterprise wide risk management, decision making support and regulatory compliance?	
2	Are there quality initiatives in terms of benchmarking and migrating industry best practices?	
3	Are there controls, procedures and policies in place in order to manage-mitigate-respond to key organizational risks ?	
4	With the increase of technology dependence and emergence of E-commerce , is the organization well equipped in integrating process, people, business and technology?	
5	In order to increase value without substantial increase in costs, can the internal audit function be outsourced ?	
6	With the increase in fraud risks as a result of increased globalization and dependence on technology, is there expertise to respond to potential fraud	

Training Material on Internal Audit

S No	Question	Management Response
	risks or frauds that might have already occurred?	
7	When stakeholder satisfaction and regulatory compliance has become indispensable in view of Revised clause 49 (in the Indian context), SOX, SAS 70 , are there systems and procedures to ensure compliance to relevant regulations/ Acts?	
8	Are there dedicated teams functioning to promote - efficiency and effectiveness of business operations - Profitability - Cost savings and value add?	
9	Are there procedures and policies in place incorporating the fundamentals of ethics pervading the general control framework within which our business operate?	
10	Does the organization require external expertise to help in Control Self Assessment?	

Chapter-IV.11

Draft Risk Management Policy (Illustrative)

Risk Management Policy

Purpose

This document sets out the organization's Risk Management Policy and includes:

- The *objectives* of Risk Management arrangements;
- *Definitions* of relevant terms;
- *Risk management principles*; and
- *Relative responsibilities*;

The Organization's '*Risk Tolerance*':

- The *Risk Framework* and how it will work; and
- How Risk Management contributes to providing an *Assurance*.

It has been approved by the Director, Chief Executive and the Director's Board.

Risk Management in the organization provides a framework to identify, assess and manage potential risks and opportunities. It provides a way for managers to make informed management decisions.

Effective Risk Management affects everyone in the organization. To ensure a widespread understanding, Board members and all operational/business unit managers should be familiar with, and all staff aware of, the principles set out in this document.

Risk Management Objectives

The objectives of this organization's Risk Management arrangements are to help managers make informed choices which:

- Improve business performance by informing and improving decision making and planning;
- Promote a more innovative, less risk averse culture in which the taking of calculated risks in pursuit of opportunities to benefit the organization is encouraged;
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance.

The improvements and benefits which effective Risk Management should provide are:

- An increased likelihood of achieving the organisation's aims, objectives and priorities;
- Prioritizing the allocation of resources;
- Giving an early warning of potential problems; and
- Providing everyone with the skills to be confident risk takers.

Definitions

The organisation's Risk Management Policy is formed around a common understanding of ***Risk Management, Risk, Corporate Risk and Operational Risk***. These are set out in Appendix 1.

The definition of risk reflects that already in circulation and used by business units at the operational level for Control and Risk Self-Assessment reviews and by Internal Audit Services for their internal audit reviews.

Risk Management Principles

The principles contained in this policy and strategy will be applied at both corporate and operational levels within the organisation.

The organisation's Risk Management Policy and Strategy will be applied to all operational aspects of the Organisation and will consider external strategic risks arising from or related to our partners in the Criminal Justice System, other government departments and the public, as well as wholly internal risks.

Other government agencies are devising and implementing Risk Management Strategies. Our organisation may impinge on their risk profile.

Our positive approach to risk management means that we will not only look at the risk of things going wrong, but also the impact of not taking opportunities or not capitalising on corporate strengths.

General Principles

All risk management activity will be aligned to corporate aims, objectives and organisational priorities, and aims to protect and enhance the reputation and standing of the organisation.

Risk analysis will form part of organisational strategic planning, business planning and investment/project appraisal procedures.

Risk management will be founded on a risk-based approach to internal control which is embedded in day to day operations of the organisation.

Our risk management approach will inform and direct our work to gain an assurance on the reliability of organisational systems and will form the key means by which the Board gains its direct assurance.

Managers and staff at all levels will have a responsibility to identify, evaluate and manage or report risks, and will be equipped to do so.

We will foster a culture which provides for spreading best practice, lessons learnt and expertise acquired from our risk management

activities across the organisation for the benefit of the entire organisation.

Principles for Managing Specific Risks

Risk Management in the organisation should be proactive and reasoned. Corporate and operational risks should be identified, objectively assessed, and, where this is the appropriate response, actively managed.

The aim is to anticipate, and where possible, avoid risks rather than dealing with their consequences. However, for some key areas where the likelihood of a risk occurring is relatively small, but the impact on the organisation is high, we may cover that risk by developing Contingency Plans, eg. our Business Continuity Plans. This will allow us to contain the negative effect of unlikely events which might occur.

In determining an appropriate response, the cost of control/risk management, and the impact of risks occurring will be balanced with the benefits of reducing risk. This means that we will not necessarily set up and monitor controls to counter risks where the cost and effort are disproportionate to the impact or expected benefits.

We also recognise that some risks can be managed by transferring them to a third party, for example by contracting out, Public Private Partnership arrangements, or possibly, but unlikely for our organisation, by insurance.

Responsibilities

All personnel have a responsibility for maintaining good internal control and managing risk in order to achieve personal, team and corporate objectives. Collectively, staff in business units need the appropriate knowledge, skills, information and authority to establish, operate and monitor the system of internal control. This requires an understanding of the organisation, its objectives, the risks it faces and the people we deal with. Everyone should be aware of the risks they are empowered to take, which should be avoided and which reported upwards.

The responsibilities of the Director, Chief Executive and the Director's Board; Operational/Business Unit Managers; the Audit Committee; and Specialist Central Functions are set out in Appendix 2.

Risk Tolerance

The Director, Chief Executive and the Board encourage the taking of controlled risks, the grasping of new opportunities and the use of innovative approaches to further the interests of the organisation and achieve its objectives provided the resultant exposures are within *the organisation's risk tolerance range*.

The organisation's Risk Tolerance can be defined by reference to the following components.

Acceptable Risks

All personnel should be willing and able to take calculated risks to achieve their own and the organisation's objectives and to benefit the organisation. The associated risks of proposed actions and decisions should be properly identified, evaluated and managed to ensure that exposures are acceptable.

Within the organisation, particular care is needed in taking any action which could:

- Impact the reputation of the organisation;
- Impact performance;
- Undermine the independent and objective review of activities;
- Result in censure/fine by regulatory bodies; or
- Result in financial loss.

Any threat or opportunity which has a sizeable potential impact on any of the above should be examined, its exposures defined and it should be discussed with the appropriate line manager. Where there is significant potential impact and high likelihood of

occurrence it should be referred to the Director's Board as a corporate risk.

Prohibited Risk Areas

Organizational policies and guidance manuals define where there are mandatory processes and procedures, e.g., the Equal Opportunities Policy, etc. Full compliance with these standards is required and confirmation of compliance will be sought in the annual Certificates of Assurance process. Non-compliance with prescribed procedures constitutes an unacceptable risk.

Some risks are acceptable provided the prescribed organisational process is followed, e.g. expenditure proposals, staff recruitment, and designated responsibilities/authorities are adhered to.

Subject to the conditions set out in Annex B to the Framework Document specifying the principles governing the relationship between Headquarters and the Area Offices, Area managers may take risk management decisions on the basis of their delegated financial authority and the devolved responsibilities set out in the Framework Document.

Risk Framework

The Board will maintain a current 'Corporate Risk Profile' as a basis for implementing and monitoring the risk management activities. This profile will include detail of the *Impact and Likelihood* of each of the risk identified, indicate *Ownership/Responsibility* and specify an *Action Plan* for treatment. This will be reviewed and updated half yearly. Progress of the risk management programme will be a standing Board agenda item.

To help to meet their responsibilities to identify, evaluate and manage operational risks, Business Unit Managers are asked by the Board to maintain:

- An Area/Divisional Risk profile which details the priority (impact and likelihood) and ownership within the Area/Division;
- A risk management action plan;

- Evidence, e.g. AMT meeting minutes, of regular review and monitoring of the profile and action plan.

Assurance

The use of this risk management approach should help to identify aspects for detailed review within the Area (for example using Control and Risk Self-Assessment) and inform and support the Area/HQ Directorate Annual Certificate of Assurance.

The Corporate Risk Profile will inform Internal Audit Services of the work necessary to provide the annual assurance. For the corporate risks identified by the Board, internal audit services will evaluate the effectiveness of the existing controls and risk management responses. The internal audit services assurance will include an assessment of the reliability and effectiveness of the organisation's overall Risk Management arrangements.

Appendix 1

Corporate Risk Management

Definitions

Risk Management is the culture, processes and structure that are directed towards the effective management of potential opportunities and threats to the organization and its contribution to the public sector.

RISK is something which could:

- Have an impact by not taking opportunities or not capitalising on corporate strengths,
- Prevent, hinder or fail to further the achievement of objectives,
- Cause financial disadvantage, i.e. additional costs or loss of money or assets; or
- Result in damage to or loss of an opportunity to enhance the organisation's reputation.

Corporate Risk is a significant risk requiring reference to and monitoring by the Director's Board, i.e. those risks assessed as having a high impact on the business of the organisation and a high likelihood of occurring.

Operational Risk is any less significant risk requiring resolution elsewhere in the organisation, i.e. risks with a medium or low impact and likelihood which are managed by business units.

Appendix 2

Corporate Risk Management

Responsibilities

1. **The Director, Chief Executive and the Director's Board** – as Accounting and additional Accounting Officers, the Director and Chief Executive are ultimately accountable for the effective management of the organisation's business and in particular for ensuring that there are adequate risk management arrangements and a sound system of internal control.
2. The Board is responsible for ensuring that corporate risks are properly managed and will require evidence that risk is being managed, and results are properly measured. Other Board responsibilities are:
 - Developing and communicating organisational policy and information about the risk management programme to all staff, and where appropriate to our partners;
 - Defining the organisation's risk tolerance (the overall level of exposure and nature of risks which are acceptable to the organisation – see section 6 below);
 - Setting policies on internal control based on the organisation's risk profile, its ability to manage the risks identified and the cost/benefit of related controls; and
 - Seeking regular assurance that the system of internal control is effective in managing risks in accordance with the Board's policies.
3. Individual members of the Board will assume ownership for managing specific corporate risks.
4. **Operational/Business Unit Managers (Area Heads and Heads of Division)** – are responsible for ensuring compliance with the prescribed procedures set out in

Training Material on Internal Audit

organisational policies. They have a responsibility to identify, evaluate and manage operational risks and bring to the Board's attention emerging corporate risks. Business unit managers are ideally placed to pick up on those early warning indicators which might identify where problems are developing and this is an important responsibility.

5. Operational managers should ensure that everyone in their unit understands their risk management responsibilities and must make clear the extent to which staff are empowered to take risks.
6. **The Audit Committee** – is responsible for advising the Director, Chief Executive and the Board on Risk Management and internal control. It is also responsible for collating the sources of assurance which inform how effectively risk is managed and the reliability of the internal control system.
7. **Specialist Central Functions** – Internal Audit Services, Business Information Services Directorate and Finance Directorate, Personnel Directorate etc. will assist managers by providing advice and support in relation to their specialisms.

**INTERNAL CONTROL
FRAMEWORK –
UNDERSTANDING AND
EVALUATION**

Chapter-V.1

Introduction to Internal Controls

“ I have never been in an accident of any sort worth speaking about.

I never saw a wreck and have never been wrecked, nor was I ever in any predicament that threatened to end in disaster of any sort”

- EJ Smith, Captain- Titanic

(1st April 1912, 11 days before the Titanic sank)

Definition

Internal controls are a system consisting of specific policies and procedures designed to provide management with *reasonable assurance* that the goals and objectives it believes important to the entity will be met.

In accounting and organizational theory, **Internal control** is defined as a process, effected by an organization's people and information technology (IT) systems, designed to help the organization accomplish specific goals or objectives. It is a means by which an organization's resources are directed, monitored, and measured. It plays an important role in preventing and detecting fraud and protecting the organization's resources, both physical (e.g., machinery and property) and intangible (e.g., reputation or intellectual property such as trademarks). At the organizational level, internal control objectives relate to the reliability of financial reporting, timely feedback on the achievement of operational or strategic goals, and compliance with laws and regulations. At the specific transaction level, internal control refers to the actions taken to achieve a specific objective (e.g., how to ensure the organization's payments to third parties are for valid services rendered.) Internal control procedures reduce process variation, leading to more predictable outcomes. Internal control is a key element of the Foreign Corrupt Practices Act (FCPA) of 1977 and

the Sarbanes-Oxley Act of 2002, which required improvements in internal control in United States public corporations. Internal controls within business entities are called **business controls**.

Fundamental Concepts:

- Internal control is a *process*. It's a means to an end, not an end in itself.
- Internal control is effected by *people* and not by policy manuals and forms.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance.
- Internal control is geared to the achievement of *objectives*:
 - *Process*... a series of action that permeate an entity's activity.
 - *People*... board of directors, management and other personnel.
 - *Reasonable assurance*... reality that decision-making is subjective and therefore, involves an element of risk.
 - *Objective*... quantification of goals.

Why have Internal Controls?

The major benefits of sound internal controls are as :

- Promote operational efficiency and effectiveness
- Provide reliable financial information
- Safeguard assets and records
- Encourage adherence to prescribed policies
- Comply with regulatory agencies

Basic Concepts on Internal Controls

- Management, not auditors, must establish and maintain the entity's controls.
- Internal controls structure should provide reasonable assurance that financial reports are correctly stated.
- No system can be regarded as completely effective.
- Should be applied to manual and computerized systems.

Examples of Some Typical Internal Control Procedures

- Hiring the right Personnel;
- Proper procedures for authorization;
- Adequate separation of duties;
- Adequate documents and records;
- Physical control over assets and records;
- Independent checks on performances.

Chapter-V.2

Nature and Types of Internal Controls, Control Objectives and Activities

Control Objectives - Objective categorization

Internal control activities are designed to provide reasonable assurance that particular objectives are achieved, or related progress understood. The specific target used to determine whether a control is operating effectively is called the *control objective*. Control objectives fall under several detailed categories; in financial auditing, they relate to particular *financial statement assertions*, but broader frameworks are helpful to also capture operational and compliance aspects:

1. **Existence (Validity):** Only valid or authorized transactions are processed (i.e., no invalid transactions)
2. **Occurrence (Cutoff):** Transactions occurred during the correct period or were processed timely.
3. **Completeness:** All transactions are processed that should be (i.e., no omissions)
4. **Valuation:** Transactions are calculated using an appropriate methodology or are computationally accurate.
5. **Rights and Obligations:** Assets represent the rights of the company, and liabilities its obligations, as of a given date.
6. **Presentation and Disclosure** (Classification): Components of financial statements (or other reporting) are properly classified (by type or account) and described.
7. **Reasonableness**-transactions or results appears reasonable relative to other data or trends.

For example, a control objective for an accounts payable function might be: *"Payments are only made to authorized vendors for goods or services received."* This is a validity objective. A typical control procedure designed to achieve this objective is: *"The accounts payable system compares the purchase order, receiving record, and vendor invoice prior to authorizing payment."*

Management is responsible for implementing appropriate controls that apply to transactions in their areas of responsibility. Internal auditors perform their audits to evaluate whether the controls are designed and implemented effectively to address the relevant objectives.

Control Activity Categorization

Control activities may also be described by the type or nature of activity. These include (but are not limited to):

- Segregation of Duties - separating authorization, custody, and record keeping roles to limit risk of fraud or error by one person.
- Authorization of Transactions - review of particular transactions by an appropriate person.
- Retention of Records - maintaining documentation to substantiate transactions.
- Supervision or Monitoring of operations - observation or review of ongoing operational activity.
- Physical Safeguards - usage of cameras, locks, physical barriers, etc. to protect property.
- Analysis of results, periodic and regular operational reviews, metrics, and other key performance indicators (KPIs).
- IT Security - usage of passwords, access logs, etc. to ensure access restricted to authorized personnel.

Control Precision

Control precision describes the alignment or correlation between a particular control procedure and a given control objective or risk. A control with direct impact on the achievement of an objective (or mitigation of a risk) is said to be more precise than one with indirect impact on the objective or risk. Precision is distinct from sufficiency; that is, multiple controls with varying degrees of precision may be involved in achieving a control objective or mitigating a risk.

Precision is an important factor in performing a SOX 404 risk assessment. After identifying specific financial reporting material misstatement risks, management and the external auditors are required to identify and test controls that mitigate the risks. This involves making judgments regarding both precision and sufficiency of controls required to mitigate the risks.

Risks and controls may be entity-level or assertion-level under the PCAOB guidance. Entity-level controls are identified to address entity-level risks. However, a combination of entity-level and assertion-level controls are typically identified to address assertion-level risks. The PCAOB set forth a three-level hierarchy for considering the precision of entity-level controls. Later guidance by the PCAOB regarding small public firms provided several factors to consider in assessing precision.

Control Objectives

- Reliability and Integrity of Information.
- Compliance with policies, plans, procedures, laws, and regulations.
- Safeguard assets.
- Economy and efficiency of operations.
- Accomplishment of organizational objectives and programs.

Key Terms in Internal Control

A few common internal control terms are described as follows:

- **Reportable condition:** Has the same meaning as the term *significant deficiency*. These two terms are used to define a significant deficiency in the design or operation of internal control that could adversely affect a company's ability to record, process, summarize, and report financial data consistent with the assertions of management in the company's financial statements. An aggregation of significant deficiencies could constitute a material weakness.
- **Material weakness:** Defined in the auditing literature as a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by errors or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned duties.
- **Compensating control:** Some organizations, by virtue of their size, are not able to implement basic controls such as segregation of duties. In these cases, it is important that management institute compensating controls to cover for the lack of a basic control, or if a basic control is not able to function for some period of time.

Internal Control Assessments

The Internal Auditors assess the 'as -is' Internal Control system within the organization and map it against a globally accepted 'standard' which is basically, an Internal Controls framework- COSO being the most widely used:

- Evaluate efficiency and effectiveness of controls.
- Recommend new controls where needed – or discontinuing unnecessary controls.
- Use of control frameworks (COSO, CoCo, Cadbury).

Training Material on Internal Audit

- Control self-assessment (CSA).

They also provide on-going education and training on risks and controls.

Types of Internal Controls

- **Preventive** – Prevents or minimizes errors / irregularities from occurring
- **Detective** - Highlight errors or irregularities after they have occurred
- **Reconstructive** - Effective backup and disaster recovery plans

Preventive and Detective Controls

Controls can be either preventive or detective. The intent of these control types are different.

Preventive controls attempt to deter or prevent undesirable acts from occurring. They are proactive controls that help to prevent a loss. Examples of preventive controls are separation of duties, proper authorization, adequate documentation, and physical control over assets.

Detective controls, on the other hand, attempt to detect undesirable acts. They provide evidence that a loss has occurred but do not prevent a loss from occurring. Examples of detective controls are reviews, analyses, variance analyses, reconciliations, physical inventories, and audits.

Both types of controls are essential to an effective internal control system. From a quality standpoint, preventive controls are essential because they are proactive and emphasize quality.

However, detective controls play a critical role by providing evidence that the preventive controls are functioning and preventing losses.

Typical Examples

A. Preventive:

- *Segregation of duties*
- *Dual cheque signing authority*
- *Purchase Policy*

B. Detective:

- *Bank reconciliation*
- *Audit*
- *Physical Verification of Fixed Assets*

C. Reconstructive:

- *Disaster Recovery Procedures*

Techniques of Internal Controls – Discussions

A – Separation / Segregation of Duties (SOD)

What is it?

Functions are divided so that no one person has control over all parts of a transaction.

- **Activities to Separate**

- Initiating/Authorizing (Approving)/Recording/Reconciling;
- Physically Controlling (Custody).

- **Examples**

- Cash Receipts/Recording Transactions/Bank Deposits/Bank Account Reconciliations.
- Supplier Database/Requisition/Order/Receipt of Goods (services)/Reconciling Accounts.

Training Material on Internal Audit

- Order/Receipt of Inventory/Maintenance of Inventory Records/Physical Inventory Count.

Each activity should be performed by a different employee:

- Cash custody should be independent of receipts, disbursements and the recording function.
- G/L personnel should be independent of custody, receipts, disbursements, and as many other activities in the transaction process as possible.
- Personnel making bank deposits should be independent of cash custody, receipts, disbursements, and bank reconciliations.

- **In Other Words**

The same person should not perform the following duties:

- Initiating and approving a purchase and receiving the goods directly,
- Collecting money and recording the payment on the books, or
- Issuing checks and reconciling bank accounts.

- **Issues**

- Two key questions are:
 - Does one person perform all parts of the transaction from initiating to reconciling the account?
 - Does someone have access to “information systems” that create a separation of duties problem?
- A simple way of looking at separation of duties is to have at least “two sets of eyes” look at a transaction.
 - Trust should not prevent a manager from separating duties. Often it is the longtime, trusted employee who

commits fraud because he/she knows the system and how to circumvent it.

- Banks will cash most checks presented for payment. Checks received and issued should be viewed like cash.
- In small departments, it is often difficult to separate duties. To compensate for this problem, some of the following actions could be employed:

Place greater emphasis on monitoring:

- Require employees to take vacation.
- Use the information system to analyze activities.
- Make sure cash transactions are recorded ASAP.

In small organizations, it is more likely there may be insufficient personnel to allow the various activities to be performed by the recommended number of independent personnel.

As separation of duties becomes less possible more emphasis must be placed on:

- Review of Supporting Documentation.
- Limiting access to facilities/assets.
- Transaction Authorization.
- Departmental Reconciliation.
- Independent verification by internal/external auditors.

B - Review Procedures

Validity

Refers to controls designed to ensure recorded transactions are those that should have been recorded.

Completeness

Refers to controls designed to ensure valid transactions are not omitted from the accounting records.

Authorization

Refers to controls intended to ensure transactions are approved before they are recorded.

Classification

Refers to controls intended to ensure transactions are recorded in the right accounts and charged/credited to the right vendor/customer.

Proper Period

Refers to controls over accounting for transactions in the period in which they occur.

C. Authorization

What is it?

Transactions are executed and access to assets is permitted only in accordance with management's directives. This is a preventive control.

Issues

- Signature authority or delegation of that authority should be limited to a "need to have" basis. It is like giving someone signed blank checks. Consequently, managers should judiciously limit authorization authority.
- "Rubber stamping" documents circumvents this control. Managers should question what they sign, at least on a sample basis. Where appropriate, supporting documentation should be attached to the signature form or at least made available. Questioning various transactions and requesting additional information enhances a control conscious environment.
- Written procedures outlining the delegation guidelines should be developed.

Information Authorization

- Access to, and use of, computing resources is restricted to appropriately authorized users.
- All means of access to automated information resources, such as passwords, are confidential and proprietary to the university. Passwords authenticate a user's identity and establish accountability.

An employee is required to maintain the privacy of his or her password(s) and is accountable for the unauthorized use. Sharing user identification codes or revealing passwords is prohibited.

D. Controls over Assets / records

What is it?

Establishing control procedures to prevent loss of physical and intellectual assets/records and assuring that assets/records are physically secured; these are preventive controls. Taking a physical inventory, on the other hand, is a detective control.

Issues

- Managers are personally responsible for the assets in their organization. Assets have a way of "walking off" if physical controls don't exist.
- Equipment moved between labs or classrooms needs to be monitored.
- Separation of duties should be maintained between the person who has custody of the assets/records and the person who takes the physical inventory.

Asset Control Activities

- Periodic asset counts
- Use of perpetual records

- Periodic comparisons of the accounting records to the perpetual records
- Investigation of discrepancies
- Periodic summaries of inventory usage
- Physical safeguards against theft and fire
- Proper authorization of purchases

E. Monitoring

Why is it Important?

- Monitoring ensures that the internal control system is operating as expected. Just because a control exists does not mean that it is properly functioning. Effective controls may be designed into the system, but are not effective unless they are functioning properly.
- Managers, for their areas, and individual employees, for their workstations, should perform ongoing monitoring activities to determine whether the control system can be relied on to provide reasonable assurance that financial and compliance goals can be accomplished and to address new risks.
- Monitoring is a detective control that aids in identifying losses, errors or irregularities.

Management's role in the internal control system is critical to its effectiveness. Managers, like auditors, don't have to look at every single piece of information to determine that the controls are functioning and should focus their monitoring activities in high-risk areas. The use of spot checks of transactions or basic sampling techniques can provide a reasonable level of confidence that the controls are functioning. Individual employees should routinely review and evaluate internal controls affecting their area of responsibility and accountability.

Monitoring Activities

- Review and evaluate financial reports for propriety and trends.

Nature and Type of Internal Controls, Control Objectives and Activities

- Review reconciliations, ensuring that reconciling items are investigated.
- Verify the propriety of supporting documentation.
- Have Internal Audit review high risk areas.
- Have periodic asset counts performed.
- Make surprise cash counts.
- Follow-up on complaints, allegations.
- Send out periodic confirmation of accounts receivable.

Monitoring by Transaction

- *Payroll*
 - Review and approve initial pay and any “changes”.
 - Review procedures for additions/deletions.
 - Review terminations to ensure they are taken off the system.
 - Review for nonstandard hours.
 - Monitor sick/vacation leave.
- *Travel*
 - Review supporting documents.
 - Personally approve.
 - Analyze by employee and related expenses.
- *Consultants*
 - Review supporting documentation of brochure, airline ticket or hotel.
 - Make a “call” if support is not available.

Reports

- Financial reports are a key monitoring tool. Below is some information that managers should obtain from their reporting system to use to monitor controls:
 - Comparison of actual to budget.
 - Comparison of the current month to the previous month.
 - Comparison of the current month to the previous year's month.
 - Year-to-date totals.
 - Special account analysis for high risk accounts.
 - Reconciliation of department/college balances to a monthly account statement.
- For easy use, the above reports should include a variance column (where appropriate) and totals should be consistent among the reports. Also, reports should be summarized to the proper level of detail.

Some thoughts on Internal Control

Roles and Responsibilities

Everyone in the organization has some role to play in the organization's internal control system. According to the COSO Framework, everyone in an organization has responsibility for internal control to some extent. Virtually all employees produce information used in the internal control system or take other actions needed to effect control. Also, all personnel should be responsible for communicating upward problems in operations, noncompliance with the code of conduct, or other policy violations or illegal actions. Each major entity in corporate governance has a particular role to play:

Management

The Chief Executive Officer (the top manager) of the organization has overall responsibility for designing and implementing effective

internal control. More than any other individual, the chief executive sets the *"tone at the top"* that affects integrity and ethics and other factors of a positive control environment. In a large company, the chief executive fulfills this duty by providing leadership and direction to senior managers and reviewing the way they're controlling the business. Senior managers, in turn, assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions. In a smaller entity, the influence of the chief executive, often an owner-manager, is usually more direct. In any event, in a cascading responsibility, a manager is effectively a chief executive of his or her sphere of responsibility. Of particular significance are financial officers and their staffs, whose control activities cut across, as well as up and down, the operating and other units of an enterprise.

Chief executive officer (CEO)

The CEO has ultimate responsibility and ownership of the internal control system. The individual in this role sets the tone at the top that affects the integrity and ethics and other factors that create the positive control environment needed for the internal control system to thrive. Aside from setting the tone at the top, much of the day-to-day operation of the control system is delegated to other senior managers in the company, under the leadership of the CEO.

Chief financial officer (CFO)

Much of the internal control structure flows through the accounting and finance area of the organization under the leadership of the CFO. In particular, controls over financial reporting fall within the domain of the chief financial officer. The audit committee should use interactions with the CFO, and others, as a basis for their comfort level on the internal control over financial reporting.

This is not intended to suggest that the CFO must provide the audit committee with a level of assurance regarding the system of internal control over financial reporting. Rather, through interactions with the CFO and others, the audit committee should get a gut feeling about the completeness, accuracy, validity, and maintenance of the system of internal control over financial reporting.

Controller/director of accounting or finance

Much of the basics of the control system come under the domain of this position. It is key that the controller understands the need for the internal control system, is committed to the system, and communicates the importance of the system to all people in the accounting organization. Further, the controller must demonstrate respect for the system through his or her actions.

Internal audit

A main role for the internal audit team is to evaluate the effectiveness of the internal control system and contribute to its ongoing effectiveness. With the internal audit team reporting directly to the audit committee of the board of directors and/or the most senior levels of management, it is often this function that plays a significant role in monitoring the internal control system. It is important to note that many not-for-profits are not large enough to employ an internal audit team. Each organization should assess the need for this team, and employ one as necessary.

The internal auditors and external auditors of the organization also measure the effectiveness of internal control through their efforts. They assess whether the controls are properly designed, implemented and working effectively, and make recommendations on how to improve internal control. They may also review Information technology controls, which relate to the IT systems of the organization. There are laws and regulations on internal control related to financial reporting in a number of jurisdictions. In the U.S. these regulations are specifically established by Sections 404 and 302 of the Sarbanes-Oxley Act. Guidance on auditing these controls is specified in PCAOB *Auditing Standard No. 5* and SEC guidance, further discussed in SOX 404 top-down risk assessment. To provide reasonable assurance that internal controls involved in the financial reporting process are effective, they are tested by the external auditor (the organization's public accountants), who are required to opine on the internal controls of the company and the reliability of its financial reporting.

Board of director/audit committee

A strong, active board is necessary. This is particularly important when the organization is controlled by an executive or management team with tight reins over the organization and the people within the organization. The board should recognize that its scope of oversight of the internal control system applies to all the three major areas of control: over operations, over compliance with laws and regulations, and over financial reporting. The audit committee is the board's first line of defense with respect to the system of internal control over financial reporting.

The board is ultimately responsible for the system of internal control. Board can delegate to management the task of establishing, operating and monitoring the system, but can not delegate their responsibility for it.

Management is accountable to the board of directors, which provides governance, guidance and oversight. Effective board members are objective, capable and inquisitive. They also have a knowledge of the entity's activities and environment, and commit the time necessary to fulfill their board responsibilities. Management may be in a position to override controls and ignore or stifle communications from subordinates, enabling a dishonest management which intentionally misrepresents results to cover its tracks. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal and internal audit functions, is often best able to identify and correct such a problem.

All other personnel.

The internal control system is only as effective as the employees throughout the organization that must comply with it. Employees throughout the organization should understand their role in internal control and the importance of supporting the system through their own actions and encouraging respect for the system by their colleagues throughout the organization.

Compensating Controls

It is important to realize that both the design and compliance with the internal control system is important. The audit committee

should be tuned-in to the tone-at-the-top of the organization as a first indicator of the functioning of the internal control system.

In addition, audit committees should realize that the system of internal control should be scaled to the organization. Some organizations will be so small, for example, that they will not be able to have appropriate segregation of duties. The message here is that the lack of segregation of duties is not automatically a material weakness, or even a reportable condition, depending on the compensating controls that are in place.

For example, suppose an organization's accounting department is so small that it is not possible to segregate duties between the person who does the accounts payable and the person who reconciles the bank statements. In this case, it is one and the same person, so the implication is that there are no checks and balances on the accounts payable person, who could be writing checks to a personal account, then passing on them during the bank reconciliation process (that is, there is no one to raise the red flag that personal checks are being written on the company account).

Compensating controls could make up for this apparent breach in the internal control system. Here are some examples of compensating controls in this situation:

1. All checks are hand signed by an officer of the company, rather than using a signature plate that is in the control of the person that prepared the checks.
2. The bank reconciliation may be reviewed by the person's manager.
3. A periodic report of all checks that are cleared at the bank could be prepared by the bank and forwarded to an officer of the company for review.

Audit committees should be aware of situations like this and be prepared to ask questions and evaluate the answers when an obvious breach in internal control is surfaced.

Management Override of Controls

Another area that an audit committee needs to focus on is the ability of management to override internal controls over financial reporting to perpetrate a fraud. Examples of techniques used by management in overriding internal controls over the financial reporting function include:

- Back dating or forward dating documents to a different period.
- Making adjusting entries during the financial reporting closing process.
- Reclassifying items improperly between the statement of activity and the statement of financial condition.

Some of these override techniques were used in some of the recent scandals and have gained substantial notoriety.

An audit committee has the responsibility to help prevent or deter a management override of controls. It is important for the audit committee to understand that there is a system to uncover an override, as well as follow-up to determine its appropriateness. Questions about management override, and the controls over management override, as well as audit steps to detect if a management override has occurred, should be addressed to the CEO, CFO, and independent auditor during the respective executive sessions with the audit committee as noted elsewhere in this toolkit.

The capabilities of an organization in relation to the COSO model could be assessed based on universal states or plateaus that organizations typically target. The descriptions are incremental. The capability descriptions are based on evolution toward generally recognized best practices. Each organization determines which level of "maturity" would be the most appropriate in support of its business needs, priorities and availability of resources. A rating system of "0" to "5" is used. A rating of "5" does not necessarily mean "goodness", but rather, maturity of capability.

The ideal maturity rating for any area is dependent on the needs of the organization. The different and progressive plateaus are:

0 Non-existent when:The organisation lacks procedures to monitor the effectiveness of internal controls. Management internal control reporting methods are absent. There is a general unawareness of IT operational security and internal control assurance. Management and employees have an overall lack of awareness of internal controls.

1 Initial/Ad Hoc when:Management recognises the need for regular IT management and control assurance. Individual expertise in assessing internal control adequacy is applied on an ad hoc basis. IT management has not formally assigned responsibility for monitoring the effectiveness of internal controls. IT internal control assessments are conducted as part of traditional financial audits, with methodologies and skill sets that do not reflect the needs of the information services function.

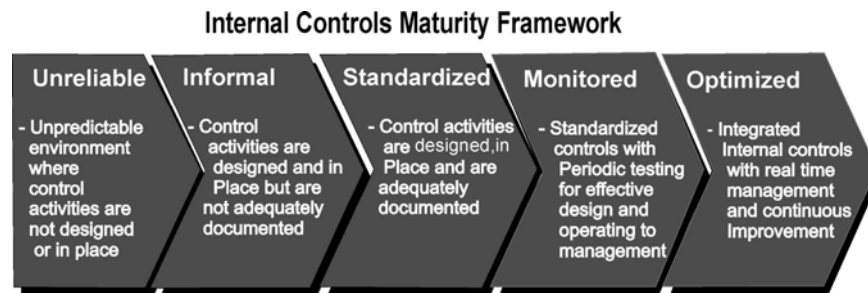
2 Repeatable but Intuitive when:The organisation uses informal control reports to initiate corrective action initiatives. Internal control assessment is dependent on the skill sets of key individuals. The organisation has an increased awareness of internal control monitoring. Information service management performs monitoring over the effectiveness of what it believes are critical internal controls on a regular basis. Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan. Risk factors specific to the IT environment are identified based on the skills of individuals.

3 Defined when:Management supports and institutes internal control monitoring. Policies and procedures are developed for assessing and reporting on internal control monitoring activities. An education and training programme for internal control monitoring is defined. A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT managers. Tools are being utilised but are not necessarily integrated into all processes. IT process risk assessment policies are being used within control frameworks developed specifically for the IT organisation. Process-specific risks and mitigation policies are defined.

4 Managed and Measurable when: Management implements a framework for IT internal control monitoring. The organisation establishes tolerance levels for the internal control monitoring process. Tools are implemented to standardise assessments and automatically detect control exceptions. A formal IT internal control function is established, with specialised and certified professionals utilising a formal control framework endorsed by senior management. Skilled IT staff members are routinely participating in internal control assessments. A metrics knowledge base for historical information on internal control monitoring is established. Peer reviews for internal control monitoring are established.

5 Optimised when: Management establishes an organisationwide continuous improvement programme that takes into account lessons learned and industry good practices for internal control monitoring. The organisation uses integrated and updated tools, where appropriate, that allow effective assessment of critical IT controls and rapid detection of IT control monitoring incidents. Knowledge sharing specific to the information services function is formally implemented. Benchmarking against industry standards and good practices is formalised

A graphic representation is as –



Chapter-V.3

Understanding Control Frameworks – COSO Model

The COSO Model of Internal Control is the most widely accepted global framework. There are however, some other models like CoCo (Canadian Organization), Turnbull Guidance etc.

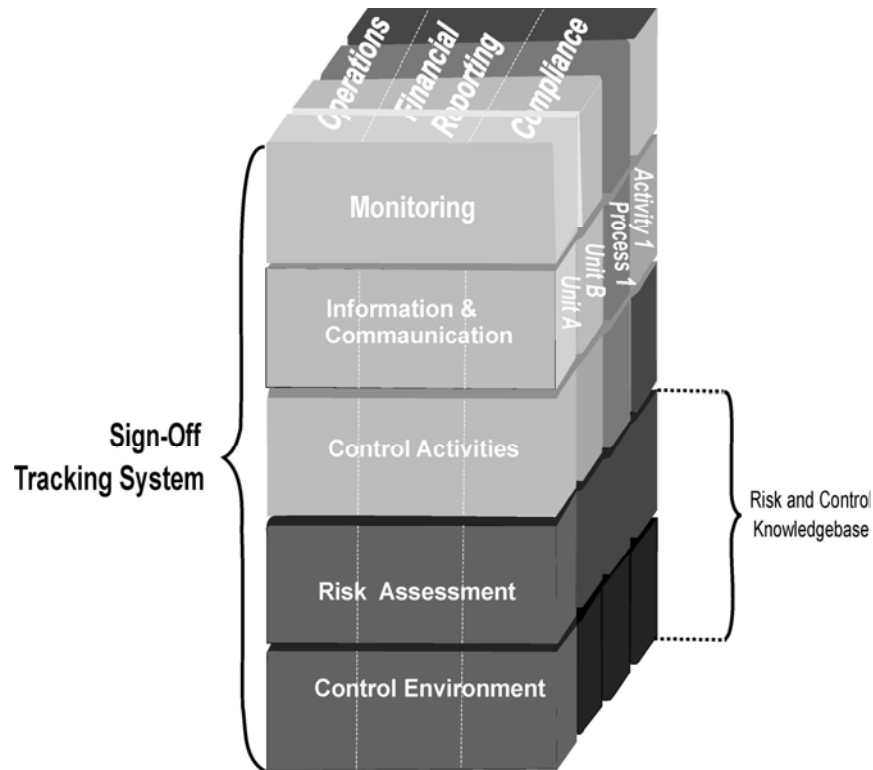
COSO Framework – Basic Facts

- COSO provides the Public Company Accounting Oversight Board (PCAOB)'s accepted basis for establishing internal control systems and determining their effectiveness.
- Stands for "Committee of Sponsoring Organizations".
- Originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (aka "The Treadway Commission").
- The sponsoring organizations include:
 - American Institute of Certified Public Accountants (AICPA).
 - The Institute of Internal Auditors (IIA).
 - Financial Executives International (FEI).
 - Institute of Management Accountants (IMA).
 - American Accounting Association (AAA).
- Published two documents and one pending.
 - 1992 – Internal Controls – Integrated Framework.
 - Mid 90's – Internal Control on Derivative Issues.
 - Early 2004 – Enterprise Risk Management Framework.

The 5-layered COSO Framework is illustrated below. However, this has been superseded by the new 8-layered structure.

The COSO 5- Layered Structure

Objectives



The COSO New 8-layered Structure



The additions to the old 5 layers–

- Internal Environment
- Objective setting
- Event identification
- Risk Response

Deleted : Risk Assessment layer

4 Top-Level Objectives – Strategic, Operations, Reporting, Compliance

Internal Control Components

- The *control environment* provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It serves as the foundation for the other components.
- Within this environment, management *assesses risks* to the achievement of specified objectives. *Control activities* are implemented to help ensure that management directives to address the risks are carried out.
- Meanwhile, relevant *information is captured and communicated* throughout the organization. The entire process is *monitored* and modified as conditions warrant.

Control Environment

- sets the tone of an organization.
- influencing the control consciousness of its people.
- foundation of all other components.
- providing discipline and structure.

Control Environment Factors

- Integrity and ethical values.
- Commitment to competence.
- Board of directors or Audit committee.
- Management philosophy and operating cycle.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.

Risk Assessment is the identification and analysis of relevant risks to achievement of the objective, forming a basis for determining how the risks should be managed.

Key Considerations

- Completeness of risk identification.
- The probability that risk will materialize.
- The potential consequences (materiality) if the risk materializes.

Control Activities

Control Activities are the policies and procedures that help ensure management directives are carried out.

Kinds of Control Activities

- **Top level reviews** actual performance versus budgets, forecasts, prior periods and competitors.
- **Direct functional or activity management.** Managers running functions or activities review performance reports.
- **Information processing** controls are performed to check accuracy, completeness and authorization of transactions.
- **Physical controls** assets are secured physically and periodically counted and compared with control records.
- **Key Performance indicators** relating different sets of data ...operating and financial together with analyses of the relationships and investigative and corrective actions.
- **Segregation of duties** are divided, or segregated, among different people to reduce the risk of error or inappropriate actions.
- **Information** must be identified, captured and communicated in a form and time frame that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance related

information that makes it possible to run and control the business.

- **Communication** is inherent in information systems. Information produced by information systems must be communicated to the appropriate personnel so that they carry out their operating, financial and compliance responsibilities.

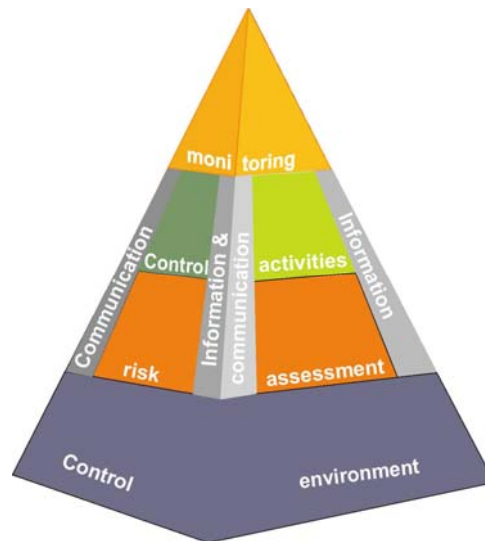
“The board should send out a clear message that control responsibilities must be taken seriously”

Monitoring

A process that assess the quality of the system's performance over time. It includes regular management and supervisory activities, and other actions personnel take in performing their duties.

Ways of Monitoring

- **Ongoing activities:** Activities that serve to monitor the effectiveness of internal control in the ordinary course of operations.
- **Separate evaluations:** using an evaluation tool and methodology that focus directly on a system's effectiveness. Such as checklists, flowcharting, questionnaires etc.



How the components fit together

“Ultimately, a company’s approach to control will depend on the board’s appetite for risk, its attitude and the corporate philosophy.”

Using a *Risk Management Diagnostic* an organization is able to challenge whether all the necessary components of an internal control system exist. Existence of all the components enables risk management to be embedded into the organization.

Internal Control Weaknesses

Most common weaknesses we see in organizations are:

- *Philosophy-* understood but not written, open to misinterpretation;
- *Roles and responsibilities-* responsibilities are not explicit throughout the organization;
- *Risk to delivering performance-* some form of risk profiling, but often divorced from practical reality of doing business;
- *Performance appetite-* lack of understanding of the organization's appetite for risk taking;
- *Summary of performance and risk effectiveness-* boards do not receive the right information, either too little or too much;
- *Behavior-* disincentives exist which lead employees to behave in a dysfunctional manner.

Internal Control - limitations

- It can help achieve performance and profitability targets.
- It can help prevent loss of resources.
- It can help ensure reliable financial reporting.
- It can help ensure compliance with laws.

- It can help an entity get to where it wants to go, and avoid pitfalls and surprises along the way

Some further Limitations

- **Cost-** the cost of the control should not exceed the benefit.
- **Only reasonable assurance-** risk can be lowered but not eliminated.
- **Judgment-** human judgments may be faulty.
- **Collusion-** collusive activities of two or more individuals can result in control failures.
- **Breakdowns-** even if controls are well designed, they can break down.
- **Management override-** overruling prescribed policies and procedures for illegitimate purposes with the intent of personal gain.

Control Self Assessments (CSA)

What is Control Assessment?

Control assessment is a formalized, documented and committed approach to the regular, fundamental and open review by managers and staff, of the strength of control systems designed and operated to achieve business objectives and guard against risks within their sphere of influence.

Operating principles and design features of control assessment program:

- Ownership of control assessment program must be with the management.
- Objectives and deadlines of the control assessment program must be clearly defined.
- Guidance and involvement of internal audit should be clearly defined.
- Must be simple to understand and implement.
- Must ultimately be a part of the management process.

Steps of a Typical CSA



CSA Approach

- Standard Audit practices using a participative style.
- Assisting managers and staff to assess their risks and control using control framework model.

This approach is based on three premises:

- People know best: the staff of an organization are best placed to provide insights into the strengths and weaknesses of their processes.
- Internal Auditors should work 'in a collegial spirit' to identify control problems and solutions.
- The use of focus groups and 'affinity process' provides one of the most efficient means of gathering substantial amounts of highly relevant and useful data.

Control Assessment Workshops

Advantages of control assessments work shops include:

- harness group knowledge.
- Identify different perspectives.
- stimulate ideas.
- form a consensus view on the issues raised.
- create group commitment to action.
- clarify operational roles and responsibilities.
- promote ownership of processes, control and change.
- highlight soft issues like business ethics, informal controls.
- build inter personal relationship.

Embedding Control Assessment as Part of the Control Framework

- Ultimate form of control assessment.
- Making managers and staff 'self starters' of control reviews.
- Auditors ensure proper allocation of control responsibilities.
- Auditors simply audit the control assessment as an embedded part of the control framework.

Chapter-V.5

IT Controls and Cobit

The essentials...

Identification

Can we find out who is trying to reach us?

Authentication

Can we ensure that the users are who they pretend to be?

Authorization

Can we limit/control their actions?

Confidentiality

Can we ensure that the privacy of sensitive information is

Integrity

Can we ensure that the data has not been manipulated during or after the transmission?

Non repudiation

Can we ensure that the sender and receiver are accountable/ responsible for their actions?

Auditability

Can we ensure the ability to trace actions?

Intrusion Detection

Can we detect any unauthorized access attempts?

Availability

Can we correct the errors as soon as they are detected?

Error Correction

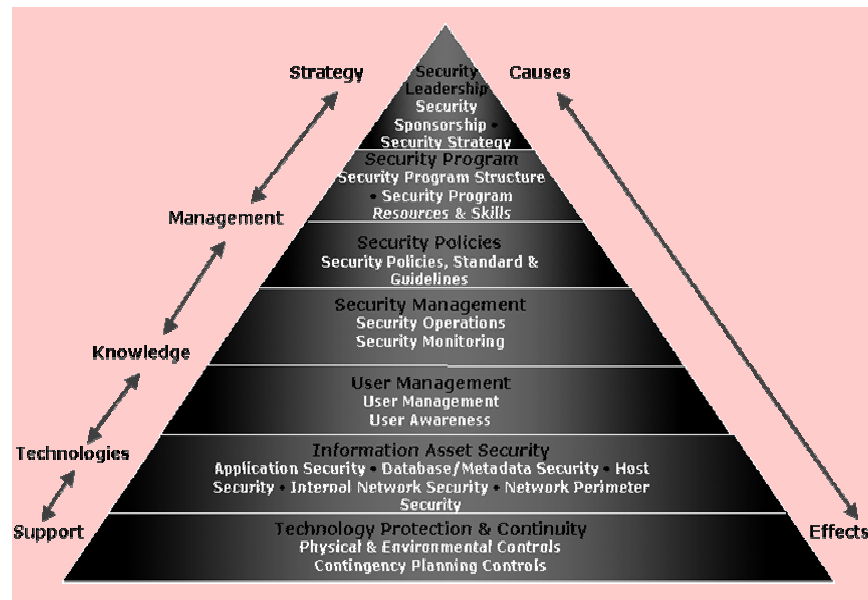
Can we ensure availability of information as required?

Key facets of IT controls include:

- **People** – organization, responsibility, accountability, and leadership
- **Process** – policies, procedures, and practices
- **Technology** – scalable technical support for automation, integration, and enabling of information security operations.

Comprehensive

Approach



Types of IT Controls

- General IT controls.
- Application controls.
- Organisation and management.
- Segregation of duties.
- Logical access controls.
- Physical access controls.
- Systems acquisition and maintenance.
- User Management.
- Computer operations.

General IT Safeguards

COSO defines IT General controls as, "Policies and procedures that help ensure the continued, proper operations of computer information systems. They include controls over data-center operations, systems software acquisition and maintenance, access security, and application system development and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer controls and information technology controls."

Illustrations of General IT safeguards

- User access tracking.
- Tracking data inserts, modifications, and deletes.
- Limiting access to necessary system areas.
- Keeping user id's and passwords secure.
- Periodically testing security roles.
- **General controls deal with the control environment** -They include all but application/transaction controls.
- **Application/transaction controls** relate to the correctness and completeness of data as well as controls over the correctness and completeness of the processing of data.

General Controls – illustrations

- **High level controls**
 - Detective.
 - Comparison and reconciliation.
 - Performed by independent people.
 - Relied upon by management.
 - Promptly followed up.

- **Low level controls**
 - Preventive.
 - Operates on single process.
 - Applies to each transaction.
 - Serves single objective.

Application Controls

COSO defines Application controls as, “Programmed procedures in application software, and related manual procedures, designed to help ensure the completeness and accuracy of information processing. Examples include computerized edit checks of input data, numerical sequence checks and manual procedures to follow up on items listed in exception reports.”

Application Controls - Illustration

- **Input controls**
 - Input validation controls.
 - Self-checking digits.
 - Use of stored reference items to eliminate input of frequently required data.
 - Debit and credit checks.
 - Authorization codes.
- **Processing controls**
 - Batch controls.
 - Reasonableness tests.
 - Access controls over programs.
 - Logic tests.
 - Telecommunication controls.

- **Output controls**
 - Managerial review.
 - Automated comparison.

Business Continuity Planning (BCP)

- **Analysis**
 - Impact Analysis.
 - Threat Analysis.
 - Documentation.
- BCP involves Solution Design ,Implementation, Testing and organization Acceptance, Maintenance. It also encompasses Information update and testing, Testing and verification of technical solutions and Testing and verification of organization recovery procedures. BCP sits alongside Disaster Recovery Planning.

Disaster Recovery Planning

- Of companies that had a major loss of computerized records,
 - 43% never reopened,
 - 51% closed within two years, and
 - only 6% survived long-term.
- Companies spend up to 25% of their IT budgets on DRP.
- 11th September 2001 attack changed the 'worst case scenario' paradigm for Disaster Recovery Planning.
- DRP process –
 - Assess business impact and risk.
 - Develop a Disaster Recovery framework.
 - Adjust information systems to make Disaster Recovery easier.

COBIT Overview

COBIT is a framework and supporting tool set that allow managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders. COBIT enables the development of clear policies and good practice for IT control throughout enterprises. COBIT is continuously kept up to date and harmonised with other standards and guidance.

Hence, COBIT has become the integrator for IT good practices and the umbrella framework for IT governance that helps in understanding and managing the risks and benefits associated with IT. The process structure of COBIT and its high-level, business-oriented approach provide an end-to-end view of IT and the decisions to be made about IT.

The **benefits of implementing COBIT** as a governance framework over IT include:

- Better alignment, based on a business focus.
- A view, understandable to management, of what IT does.
- Clear ownership and responsibilities, based on process orientation.
- General acceptability with third parties and regulators.
- Shared understanding amongst all stakeholders, based on a common language.
- Fulfilment of the COSO requirements for the IT control environment.

Successful organizations understand the benefits of information technology (IT) and use this knowledge to drive their shareholders' value. They recognize the critical dependence of many business processes on IT, the need to comply with increasing regulatory compliance demands and the benefits of managing risk effectively. To aid organizations in successfully meeting today's business challenges, the IT Governance Institute (ITGI) has published version COBIT 4.1.

COBIT 4.1 can be used to enhance work already done based upon earlier versions; it does not invalidate that previous work. When major activities are planned for IT governance initiatives, or when an overhaul of the enterprise control framework is anticipated, it is recommended to start fresh with the most recent version of COBIT.

Executive Overview of Cobit 4.1

For many enterprises, information and the technology that supports it represent their most valuable, but often least understood, assets. Successful enterprises recognise the benefits of information technology and use it to drive their stakeholders' value. These enterprises also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on information technology (IT).

The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now understood as key elements of enterprise governance. Value, risk and control constitute the core of IT governance.

IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.

Furthermore, IT governance integrates and institutionalises good practices to ensure that the enterprise's IT supports the business objectives. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage. These outcomes require a framework for control over IT that fits with and supports the Committee of Sponsoring Organisations of the Treadway Commission's (COSO's) *Internal Control—Integrated Framework*, the widely accepted control framework for enterprise governance and risk management, and similar compliant frameworks.

Training Material on Internal Audit

Organisations should satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management should also optimise the use of available IT resources, including applications, information, infrastructure and people. To discharge these responsibilities, as well as to achieve its objectives, management should understand the status of its enterprise architecture for IT and decide what governance and control it should provide.

Control Objectives for Information and related Technology (COBIT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

For IT to be successful in delivering against business requirements, management should put an internal control system or framework in place.

The COBIT control framework contributes to these needs by:

- *Making a link to the business requirements*
- *Organising IT activities into a generally accepted process model*
- *Identifying the major IT resources to be leveraged*
- *Defining the management control objectives to be considered*

The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners.

The process focus of COBIT is illustrated by a process model that subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help identify the resources essential for process success, i.e., applications, information, infrastructure and people.

In summary, to provide the information that the enterprise needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

But how does the enterprise get IT under control such that it delivers the information the enterprise needs? How does it manage the risks and secure the IT resources on which it is so dependent? How does the enterprise ensure that IT achieves its objectives and supports the business?

First, management needs control objectives that define the ultimate goal of implementing policies, plans and procedures, and organisational structures designed to provide reasonable assurance that:

- Business objectives are achieved
- Undesired events are prevented or detected and corrected

Second, in today's complex environments, management is continuously searching for condensed and timely information to make difficult decisions on value, risk and control quickly and successfully. What should be measured, and how? Enterprises need an objective measure of where they are and where improvement is required, and they need to implement a management tool kit to monitor this improvement.

The assessment of process capability based on the COBIT maturity models is a key part of IT governance implementation. After identifying critical IT processes and controls, maturity modelling enables gaps in capability to be identified and demonstrated to

management. Action plans can then be developed to bring these processes up to the desired capability target level. Thus, COBIT supports IT governance by providing a framework to ensure that:

- IT is aligned with the business.
- IT enables the business and maximises benefits.
- IT resources are used responsibly.
- IT risks are managed appropriately.

IT Governance Focus Areas

Strategic alignment focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.

- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

Illustrations on Internal Control

Illustration -1

Internal Controls in a Sales Cycle

A typical sales/accounts receivables transaction may involve the following activities:

- Credit
- Sales
- Accounts Receivable
- Inventory/Shipping
- Billing
- Cash Receipts
- Bank Deposits
- Bank Reconciliation

Some Recommended Controls

- Restrictive endorsements are placed on checks and a list of payments received is prepared.
- Payments received list is verified against daily deposit and cash receipts journal.
- Pre-numbered transactional documents are prepared for each sale transaction.
- Statements/billings are generated at least monthly.
- Personnel independent of the sales cycle review/authorize customer discounts, refunds, and credit memos.
- Aged accounts receivable are reviewed by supervisory personnel at least monthly.

Illustration - 2

Internal Controls in a Purchase Cycle

A typical purchasing/accounts payable transaction may involve the following activities:

- Ordering
- Purchasing
- Accounts Payable
- Receiving/Inventory
- Cash Disbursements
- Bank Reconciliation

Some Recommended Controls

- Pre-Numbered documents (requisitions, purchase order, invoices, etc) are utilized.
- All purchases are completed utilizing an authorized document.
- Receiving report is prepared for the receipt of all goods.
- Invoice processing matches purchase order, receiving report, and vendor invoice prior to payment processing.
- Personnel independent of the purchasing cycle review/authorize vendor discounts, refunds, and credit memos.
- Two signatures required on warrants, sight drafts, or checks over a stated amount.
- Vendor Invoices sent directly to the A/P or Accounting Department.

Illustration – 3

Internal Control Safeguards (General Controls)

- Organizational Chart up to date.

- Ethics and policies have been documented and adopted.
- Documented Procedures.
- Employees who handle cash, checks, etc. are monitored closely.
- Vacations are required.
- Budgets are used and variances investigated.
- Special entries require management approval.
- Reports issued to departments for monthly reconciliation.

Steps to enhance Internal Control

- provide financial reporting and internal control expertise, along with oversight on such matters.
- Establish a “Whistle-Blower” policy to provide the means and safeguards to those who identify fraudulent practices.
- Assess the risk associated with the processes that make-up your organization (ie., sales/revenue, cash, accounts receivable, fixed assets, accounts payable, payroll, etc.).
- For high risk areas and processes ask yourself, “What Could Go Wrong” and address the answers to the question (ie., segregation of duties).

Factors to be considered in determining the internal control policies:

- the nature and extent of risks facing the company;
- the extent and categories of risks acceptable to the company;
- the likelihood of the risks concerned materializing;
- ability to reduce and impact of risks on business; and
- the costs of operating controls relative to the benefit.

Internal Control and SOX

Sarbanes-Oxley Section 302: Internal Control Certifications

Under Sarbanes-Oxley, two separate certification sections came into effect—one civil and the other criminal.

- Section 302- (civil provision);
- Section 906- (criminal provision).

Section 302 of the Act mandates a set of internal procedures designed to ensure accurate financial disclosure. The signing officers must certify that they are “responsible for establishing and maintaining internal controls” and *“have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared.”*

PCAOB’s AS No.5

The recently released Auditing Standard No. 5 of the PCAOB, which superseded Auditing Standard No 2., has the following key requirements for the external auditor:

- Assess both the design and operating effectiveness of selected internal controls related to significant accounts and relevant assertions, in the context of material misstatement risks;
- Understand the flow of transactions, including IT aspects, sufficiently to identify points at which a misstatement could arise;
- Evaluate company-level (entity-level) controls, which correspond to the components of the COSO framework;

- Perform a fraud risk assessment;
- Evaluate controls designed to prevent or detect fraud, including management override of controls;
- Evaluate controls over the period-end financial reporting process;
- Scale the assessment based on the size and complexity of the company;
- Rely on management's work based on factors such as competency, objectivity, and risk;
- Evaluate controls over the safeguarding of assets; and
- Conclude on the adequacy of internal control over financial reporting.

The officers must “have evaluated the effectiveness of the company’s internal controls as of a date within 90 days prior to the report” and “have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.”

SOX Section 404 rules require each annual report to contain an internal control report which shall state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and contain an assessment of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Client management must:

- Document and test the internal controls over financial reporting.
- Issue an annual assertion on the effectiveness of internal control over financial reporting.

External Auditors must:

- Determine nature, timing, and extent of testing.
- Review work performed by management.
- Perform some independent tests of controls.
- Attest and report on:
 - Management's 404 assertion process.
 - Design and effectiveness of internal controls.

In order to make the assertion, the client must :

- Document and evaluate the design of controls.
- Evaluate the operating effectiveness of significant controls.
- Identify significant deficiencies or material weaknesses.
- Document the results of the evaluation.
- Communicate findings (e.g., significant deficiencies and material weaknesses) to the independent auditor.

Note: *Absence of sufficient evidence to support the Company's assessment may constitute a significant deficiency that results in a report qualification by the external auditors.*

Chapter-V.8

Control Evaluation Matrix

Evaluation of Internal Control Effectiveness

- Is the control operating as designed?
- Is the person operating the control qualified to do so effectively?
- Does the person have the necessary authority?
- How should management assess this?

Documenting Understanding and Evaluation of Internal Controls

- Narratives.
- Flowcharts.
- Questionnaires.
 - All no answers are weaknesses.
 - Look for mitigating controls elsewhere.
 - Insufficient by itself.

Important Aspects in a Process Walkthrough

- Confirm process flow.
- Confirm understanding of design.
- Confirm that understanding is complete.
- Evaluate the effectiveness of the design.
- Confirm that controls are placed in operation.

Training Material on Internal Audit

- Walkthrough does not involve testing!
- Ask personnel about their understanding of the procedures they perform.
- Determine whether personnel understand WHY they perform them.
- Determine whether they understand an exception and how to deal with it.
- Determine whether the activity is done in a timely manner.
- View documentation of a transaction flowing through the process.
- Confirm that the personnel perform the procedure as outlined in the documentation.

Control Evaluation Matrix (Illustrative only)

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
1	Integrity and Ethical Values	A code of conduct and other policies exist regarding acceptable business practices, conflicts of interest, or expected standards of ethical and moral behaviour.				
2	Integrity and Ethical Values	Employees clearly understand what behaviour is acceptable and unacceptable under the company's code of conduct and know what to do when they encounter improper behaviour.				
3	Integrity and Ethical Values	There is an established "tone-at-the-top" including explicit guidance about what is right and wrong. This tone is communicated and practiced by executives and management				

Training Material on Internal Audit

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
		throughout the organization. Executives and management continually demonstrate, through words and actions, a commitment to high ethical standards.				
4	Integrity and Ethical Values	Employees receive and understand the message that integrity and ethical values cannot be compromised. Employees are aware of what to do when they encounter improper behavior.				
5	Integrity and Ethical Values	Management follows ethical guidelines in dealing with employees, suppliers, customers, investors, creditors, insurers, competitors, regulators and auditors.				
6	Integrity and Ethical	The importance of high ethics and				

Control Evaluation Matrix

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
	Values	internal controls is discussed with newly hired employees through orientations or interviews.				
7	Integrity and Ethical Values	Management removes or reduces incentives or temptations that might cause personnel to engage in dishonest or unethical acts.				
8	Integrity and Ethical Values	Management monitors departures from approved policies and procedures or violations of the code of conduct and takes appropriate disciplinary action.				
9	Integrity and Ethical Values	Situations involving pressure to meet unrealistic targets do not exist or are properly controlled particularly for shortterm results.				

Training Material on Internal Audit

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
10	Integrity and Ethical Values	Individual compensation awards are in line with the ethical values of the company, and foster an appropriate ethical tone (e.g., bonuses are not given to those that meet objectives, but in the process circumvent established policies, procedures or controls).				
11	Integrity and Ethical Values	Codes are comprehensive and address conflicts of interest, illegal or other improper payments, anti-competitive guidelines and insider trading.				
12	Integrity and Ethical Values	Codes are periodically acknowledged by all employees.				

Control Evaluation Matrix

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
13	Integrity and Ethical Values	If a written code of conduct does not exist, management's culture emphasizes the importance of integrity and ethical behaviour by communicating orally in staff meetings, in one-on-one interface, and by example when dealing with day-to-day activities.				
14	Integrity and Ethical Values	Management and/or legal counsel monitors changes in significant laws and regulations that affect the business, and implements any appropriate changes in company policies or business practices in a timely manner.				
15	Integrity and Ethical Values	A register and record of complaints is maintained regarding significant laws with which the company is required to comply within its particular industry.				

Training Material on Internal Audit

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
16	Integrity and Ethical Values	Periodic representation is obtained from executives and other employees concerning compliance with laws and regulations.				
17	Integrity and Ethical Values	Actual losses arising from violations of laws and regulations are regularly identified, measured, and reported.				
18	Integrity and Ethical Values	Management provides guidance on the situations and frequency with which intervention of established controls may be needed.				
19	Integrity and Ethical Values	Management intervention of established controls is documented and appropriately explained.				
20	Integrity and Ethical Values	Deviations from established policies and procedures is				

Control Evaluation Matrix

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
		investigated and documented.				
21	Commitment to Competence	Company personnel have the competence and training necessary for their assigned duties.				
22	Commitment to Competence	Personnel are cross-trained to understand other functions and the impact of their specific duties on other areas of the company.				
23	Commitment to Competence	Management possesses broad functional experience (i.e., management comes from several functional areas rather than just a few, such as production and sales).				
24	Commitment to Competence	Management provides personnel with access to training programs on relevant topics.				

Training Material on Internal Audit

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
25	Commitment to Competence	Formal job descriptions or other means of defining tasks that comprise particular jobs exist and are effectively used.				
26	Commitment to Competence	Management must specify the level of competence needed for particular jobs, and translate the desired levels of competence into requisite knowledge and skills.				
27	Commitment to Competence	Adequate staffing levels are maintained to effectively perform required tasks. Employees have the requisite skill levels relative to the size of the entity and nature and complexity of activities and systems.				

Control Evaluation Matrix

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
28	Board of Directors or Audit Committee	Board committees exist. This independent governing body provides oversight for management's activities.				
29	Board of Directors or Audit Committee	Existing committees are sufficient in subject matter and membership to adequately deal with important issues.				
30	Board of Directors or Audit Committee	If an audit committee exists, a charter outlining its duties and responsibilities also exists.				
31	Board of Directors or Audit Committee	The audit committee meets privately with the chief accounting officer, internal auditors and external auditors to discuss the reasonableness of the financial reporting process, system of internal control, significant				

Training Material on Internal Audit

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
		comments and recommendations, and management's performance.				
32	Board of Directors or Audit Committee	The audit committee reviews the scope of activities of the internal and external auditors at least annually.				
33	Board of Directors or Audit Committee	A process exists for informing the board of significant issues.				
34	Board of Directors or Audit Committee	Information is communicated to the board in a timely manner.				
35	Board of Directors or Audit Committee	The compensation committee approves all management incentive plans tied to performance.				
36	Board of Directors or Audit Committee	The compensation committee, in joint consultation with the audit committee, deals with				

Control Evaluation Matrix

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
		compensation and retention issues regarding the chief internal auditor.				
37	Management's Philosophy and Operating Style	Management analyzes the risks and potential benefits of ventures.				
38	Management's Philosophy and Operating Style	Turnover in management or supervisory personnel is monitored and the reasons for significant turnover is evaluated.				
39	Management's Philosophy and Operating Style	Senior management maintains contact with and consistently emphasizes appropriate behavior to operating personnel.				
40	Management's Philosophy and Operating Style	Management exemplifies attitudes and actions reflecting a sound control environment and commitment to ethical values				

Training Material on Internal Audit

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
		including financial reporting as it relates to appropriate resolution of disputes over application of accounting treatments.				
41	Management's Philosophy and Operating Style	Management adopts accounting policies that best reflect the economic realities of the business.				
42	Management's Philosophy and Operating Style	Management has established procedures to prevent unauthorized access to, or destruction of, documents, records, and assets.				
43	Organizational Structure	Executives clearly understand their responsibility and authority for business activities and how they relate to the entity as a whole. Executives should possess the requisite experience and levels of knowledge to properly execute their positions.				

Control Evaluation Matrix

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
44	Organizational Structure	The entity establishes appropriate lines of reporting, giving consideration to its size and the nature of its activities.				
45	Organizational Structure	The structure of the entity facilitates the flow of information to appropriate people in a timely manner, including reliable and timely disclosure of material information, monitoring the performance of the disclosure infrastructure and effective flows of material information to the group responsible. The organizational structure should not be so simple that it cannot adequately monitor the enterprise's activities nor so complex that it inhibits the necessary flow of information.				

Training Material on Internal Audit

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
46	Organizational Structure	Incompatible duties are segregated (e.g., separation of accounting for and access to assets).				
47	Organizational Structure	There is an appropriate assignment of responsibility and delegation of authority to deal with organizational goals and objectives, operating functions and regulatory requirements.				
48	Assignment of Authority and Responsibility	There is a structure for assigning ownership of information including who is authorized to initiate or change transactions.				
49	Assignment of Authority and Responsibility	Employees throughout the entity are assigned authority and responsibility related to their specific job functions.				

Control Evaluation Matrix

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
50	Assignment of Authority and Responsibility	Job descriptions contain specific references to control-related responsibilities.				
51	Assignment of Authority and Responsibility	Employees are empowered, when appropriate, to correct problems or implement improvements.				
52	Assignment of Authority and Responsibility	Responsibility and delegation of authority are assigned to deal with organizational goals and objectives, operating functions, and regulatory requirements, including information systems and authorization for changes.				
53	Assignment of Authority and Responsibility	There are policies and procedures for authorization and approval of transactions.				

Training Material on Internal Audit

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
54	Assignment of Authority and Responsibility	The board of directors and/or audit committee gives adequate consideration to understanding how management identifies, monitors and controls business risks affecting the organization (i.e., strategic, operational, financial and disclosure risk).				
55	Human Resources Policies and Procedures	Management establishes and enforces standards for hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behaviour.				
56	Human Resources Policies and	Screening procedures, including background checks,				

Control Evaluation Matrix

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
	Procedures	are employed for job applicants, particularly for employees with access to assets susceptible to misappropriation.				
57	Human Resources Policies and Procedures	Recruiting practices include formal, in-depth employment interviews and informative, insightful presentations on the entity's history, culture, and operating style.				
58	Human Resources Policies and Procedures	Training policies communicate prospective roles and responsibilities and illustrate expected levels of performance and behaviour.				
59	Human Resources Policies and Procedures	Job performance is periodically evaluated and reviewed with each employee.				
60	Human Resources	Disciplinary actions send a message that				

Sr. No.	COSO Attribute	Point of Focus/Control Objective	Does this control exist? Yes / No / Partial	Control Weakness noted by auditor	Work Paper Ref. No.	Management Comments and action plan
	Policies and Procedures	violations of expected behaviour will not be tolerated.				
61	Human Resources Policies and Procedures	An ongoing education process enables people to deal effectively with evolving business environments.				

Reportable conditions relating to Internal Control

Reportable Conditions

Deficiencies in Internal Control Design

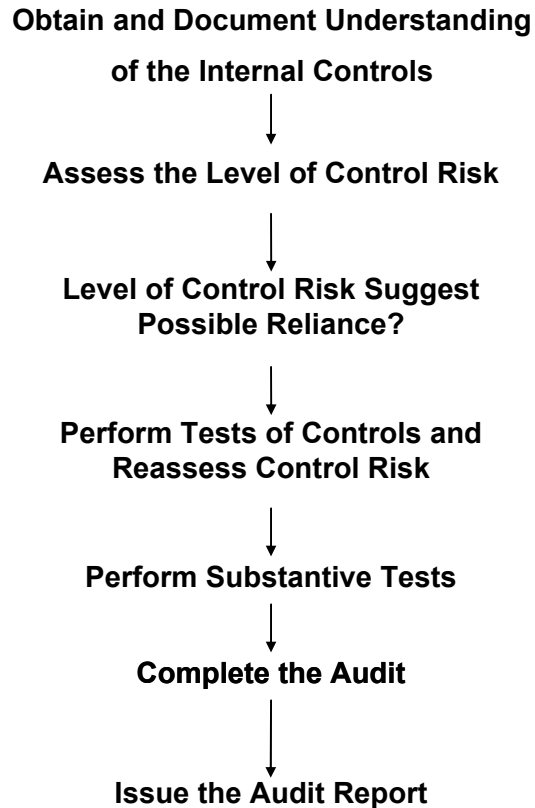
- Inadequate overall internal control design.
- Absence of appropriate segregation of duties consistent with appropriate control objectives.
- Absence of appropriate reviews and approvals of transactions, accounting entries, or systems output.
- Inadequate procedures for appropriately assessing and applying accounting principles.
- Inadequate provisions for safeguarding assets.
- Absence of other control techniques considered appropriate for the type and level of transactions activity.

- Evidence that a system fails to provide complete and accurate output that is consistent with objectives and current needs because of design flaws.
- Evidence of failure of identified controls to prevent or detect misstatements of accounting information.
- Evidence that a system fails to provide complete and accurate output consistent with the entity's control objectives because of the misapplication of control procedures.
- Evidence of failure to safeguard assets from loss, damage or misappropriation.
- Evidence of intentional override of the internal control by those in authority to the detriment of the overall objectives of the system.
- Evidence of failure to perform tests that are part of the internal control, such as reconciliations not prepared or not prepared on a timely basis.
- Evidence of willful wrongdoing by employees or management.
- Evidence of manipulation, falsification, or alteration of accounting records or supporting documents.
- Evidence of intentional misapplication of accounting principles.
- Evidence of misrepresentation by client personnel to the auditor.
- Evidence that employees or management lacks the qualifications and training to fulfill their assigned functions.
- Absence of a sufficient level of control consciousness within the organization.
- Failure to follow up and correct previously identified internal control deficiencies.

Training Material on Internal Audit

- Evidence of significant or extensive undisclosed related-party transactions.
- Evidence of undue bias or lack of objectivity by those responsible for accounting decisions.

Overview of the flow of Control Assessment and Audit



COSO Internal Control Checklists

Assessing the Effectiveness of Internal Control

Risk Assessment

- Does the company have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans include measurable performance targets and indicators?
- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis?
- Is there a clear understanding by management and others within the company of what risks are acceptable to the board?

Control Environment and Control Activities

- Does the board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks?
- Do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control system?
- Does senior management demonstrate, through its actions as well as its policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company?

- Are authority, responsibility and accountability defined clearly such that decisions are made and actions taken by the appropriate people?

Information and Communication

- Do management and the board receive timely, relevant and reliable reports on progress against business objectives and the related risks that provide them with the information, from inside and outside the company, needed for decision-making and management review purposes?
- Are information needs and related information systems reassessed as objectives and related risks or as reporting deficiencies are identified?
- Are periodic reporting procedures, including half yearly and on reporting, effective in communicating a balanced and understandable account of the companies' position and prospects?
- Are there established channels of communication for individuals to report suspected breaches of laws or regulations or others?

Monitoring

- Are there ongoing processes embedded within the company's overall business operations, and addressed by senior management, which monitor the effective application of the policies, processes and activities related to internal control and risk management?
- Do these processes monitor the company's ability to re-evaluate risks adjust controls effectively in response to changes in its objectives, its business and its external environment?
- Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to change in risk and control assessments?

- Is there appropriate communication to the board or board committees on the effectiveness of the ongoing monitoring processes on risk and control matters?
- Are there specific arrangements for management monitoring and reporting to the board on risk and control matters of particular importance?

Philosophy and Policy

- Is organization's risk management philosophy and policy clearly defined, communicated and endorsed by the board?
- Are there clearly defined roles and responsibilities for the identification, management and reporting of risk.

Behavior

- Are those responsible for risk provided with appropriate formal training?
- Do employees manage the company's risk profile in preference to their own?
- Is there independent monitoring of the overall risk management process?
- Does the organization learn from risk events when things go wrong rather than seek retribution?

Converting Strategy to Business Objectives

- Do business objectives reflect strategy?
- Are business objectives clearly communicated?

Roles and Responsibilities

- Are roles and responsibilities of all the constituent parties bought into practice by those responsible?
- Is the responsibility for reporting clearly defined?

- Are the responsibilities written into all relevant employee job descriptions?

Demonstrating of Performance and Risk Effectiveness

- Is the board provided with a clear picture of performance?
- Are Key performance indicators (KPIs) independently reviewed?
- Are KPIs clearly defined and measured?

Performance Appetite

- Is the organization's risk appetite explicitly and clearly defined?
- Is the performance of the lines of business adjusted to reflect the risks faced?
- Are action plans developed to move the organization to a more desired risk profile?

Chapter-V.10

SAS 70, Audits and Internal Control

SAS 70 Overview

Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SAS No. 70 ("SAS 70 Audit") is widely recognized, because it represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting.

SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. The issuance of a service auditor's report prepared in accordance with SAS No. 70 signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. The service auditor's report, which includes the service auditor's opinion, is issued to the service organization at the conclusion of a SAS 70 examination.

Training Material on Internal Audit

SAS No. 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report (see below). SAS 70 does not specify a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 Audit is not a "checklist" audit.

SAS No. 70 is generally applicable when an independent auditor ("user auditor") is planning the financial statement audit of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that impact a user organization's system of internal controls could be application service providers, bank trust departments, claims processing centers, data centers, third party administrators, or other data processing service bureaus.

In an audit of a user organization's financial statements, the user auditor obtains an understanding of the entity's internal control sufficient to plan the audit as required in SAS No. 55, *Consideration of Internal Control in a Financial Statement Audit*. Identifying and evaluating relevant controls is generally an important step in the user auditor's overall approach. If a service organization provides transaction processing, data hosting, IT infrastructure or other data processing services to the user organization, the user auditor may need to gain an understanding of the controls at the service organization in order to properly plan the audit and evaluate control risk.

Service Auditor's Reports One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2003). A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service

organization's controls over a minimum six month period (e.g. January 1, 2003 to June 30, 2003). The contents of each type of report is described in the following table:

Report Contents	Type I Report	Type II Report
1. Independent service auditor's report (i.e. opinion).	Included	Included
2. Service organization's description of controls.	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other information provided by the service organization (e.g. glossary of terms).	Optional	Optional

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.

In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

Benefits to the Service Organization Service organizations receive significant value from having a SAS 70 engagement performed. A Service Auditor's Report with an unqualified opinion

that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities. A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).

Without a current Service Auditor's Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources. A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user auditor's requirements.

SAS 70 engagements are generally performed by control oriented professionals who have experience in accounting, auditing, and information security. A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

Benefits to the User Organization User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls. The user organization receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

User organizations should provide a Service Auditor's Report to their auditors. This will greatly assist the user auditor in planning the audit of the user organization's financial statements. Without a Service Auditor's Report, the user organization would likely have to incur additional costs in sending their auditors to the service organization to perform their procedures.

Internal Controls and Fraud

The effects of excessive Risks and excessive Controls can have the following outcomes.

Excessive Risks

- Loss of Assets,
- Poor Business Decisions,
- Non-compliance,
- Increased Regulations, and
- Public Scandals.

Excessive Controls

- Increased Bureaucracy.
- Reduced Productivity.
- Increased Complexity.
- Increased Cycle Time.
- Increase of Non-value Activities.

Although fraud is an infrequent occurrence, we should each be aware of its possible existence. Here are some of the factors that can result in the occurrence of fraud:

Motive

- Greed.
- Financial crisis.
- Gambling/drinking/ drugs.

Training Material on Internal Audit

- Living beyond means.
- Affairs.
- Mid-life crisis.
- Revenge.
- Unappreciated.
- Workaholic.
- Family Problems.

Justification

- “It was so easy.”
- “They don’t pay me enough.”
- “My child is sick.”
- True crisis, divorce, etc.
- “My boss circumvents the rules.”
- “I’ll pay it back.”

Opportunity

- Poor or weak internal control system.
- Lack of monitoring the controls.
- High management turnover.

Below are some **indications** that fraud might be or is actually occurring:

1. Employee won’t take a vacation.
2. Unexplained variances.
3. Complaints.

4. No reconciliation to university accounting records.
5. Even amounts on checks/documents.
6. Missing reports/documents.
7. Failure to investigate reconciling items.
8. One employee “does it all”.
9. Duplicate payments or documentation is not original.
10. Using “exemptions” to use particular vendor over and over.

Questions to ask to assess Control Effectiveness and Fraud Risk

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we most vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or assets with alternative use?
- How could someone steal from the department?
- How could someone disrupt our operations?
- On what information do we most rely?
- On what do we spend the most money?
- How do we bill and collect our revenue?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?

Training Material on Internal Audit

- What is our greatest legal exposure?
- What types of transactions in our area provide the most risk?
- How can someone bypass our internal controls?

Consider various external and internal risk factors such as:

- Changing economic and political conditions.
- New technology.
- New accounting standards.
- Changing customer demands.
- Competitor actions.
- New personnel.
- The threat of outsourcing.
- New or modified information systems.
- Past performance.
- Vendor/Contractor performance and reliability.
- New products or activities.
- Reorganization

**INTERNAL AUDIT OF
SPECIFIC FUNCTIONS :
FINANCE AND ACCOUNTS,
PRODUCTION,
MARKETING,
INFORMATION
TECHNOLOGY, HUMAN
RESOURCES**

Internal Audit of Production and Operations

Operational Audit

Generic Outline of Process to Follow (applicable to internal audits of all other functions like HR, FandA, IT etc)

Step 1. Brainstorm

Brainstorm Objective of the Audit

Step 2. Set Audit Objectives

Purpose

To ensure that sufficient appropriate audit evidence will be obtained There are three elements to be identified:

Criteria / benchmark

- What will the operation to be audited be judged against (eg. policy manuals, laws, professional standards, etc)

Cause

- What are the reasons for the differences between the criteria and what the auditor will find

Effect

- What is the result or impact of this difference between the criteria and audit findings

The audit objectives will usually be posed as a question. For Example Have bulk purchases of stationary been made in excess (cause) of actual and current industry norms (criteria) thereby increasing storage and other costs (effect).

We need to Review and update the audit objectives after the preliminary survey.

Step 3. Set Scope

Purpose

To manage expectations on what will be achieved by the internal audit by setting the boundaries of what will and will not be included. Need to Review and update if necessary, but we need to ensure that this is communicated to all concerned with the management and results of the audit.

Step 4. Background Information Search

Purpose

To obtain a broad knowledge of the subject of the audit.

Offsite Background Information Search

- Nature of the operation.
- Objective of the operation.
- Operating Standards.
- Operating/budget reports.
- Seasonal time constraints.

Information Sources

- Senior Management.
- Prior Audit Papers.
- Files and Records Libraries,
- Trade journals etc.
- Industry Consultants.
- Relevant Legislation.

Step 5. Preliminary Survey

Purpose

To gain a working knowledge of the production process / operation to be audited.

To logically investigate and evaluate all information, a plan for the preliminary survey should be followed. It may be as follows:

1. ***Gain information on overall business operations*** - industry information (risks, competition, standards, special practices) - who depends on the operation's output - time and seasonal constraints - trends (staff turnover, work volumes etc) - media reports - major changes in the organisation - the size of revenue and receipts for risk areas- business recovery and business plans.
2. ***Develop a questionnaire for interviews and discussions.***
3. ***Arrange for the initial meeting (setting co- operative, but no-nonsense atmosphere).***
4. ***Interview people involved in the production and operation-*** client comments
5. ***Decide what information to obtain (on the organisation, planning, directing and controlling activities.)***
6. ***Learn the objectives, goals, and standards of the operation:***
 - how does the organisation set it's priorities?
 - standards must be assessed from the client's viewpoint, not the auditor's as that may result in assessment based on different criteria from the client's.
 - policy manuals, directives and correspondence and reports - what performance indicators are used to measure success.
7. ***Ascertain any initial opportunities for improvement.***

8. ***Learn the risks inherent in the production process / operation*** - key controls needed to counter these - influential environmental aspects.
9. ***Learn about the management of the operation*** - management style and level of control. How they find out about the work environment - specific concerns of management.
10. ***Learn about the people performing the operation***
 - key staff and their roles in the entity - written job descriptions for staff - what staff training is given? What methods are used to evaluate staff?
11. ***Carry out physical inspections***
 - tour the entity to gain overview and identify obvious areas of concern.
 - walk through a few representative work activities.
12. ***Develop formal or informal flow charts of the operating process***
13. ***Focus on possible cost savings from inefficiencies***

Developing a plan for the audit –

- **Plan** Audit resources and expertise required
- Timing of the Audit.
- Audit tests to be made and the use CAATs Audit programme.
- Risks to the audit itself.
- Major audit milestones.

Step 6. Review of Internal Controls

Purpose

To determine what level of reliance can be placed on internal controls.

This step takes place throughout the audit process.

Internal Control Review Methods

- A) Complete the Internal Control Questionnaire from interviewing staff - this gets yes or no answers to control questions, indicating areas of control weakness to concentrate on.
- B) Prepare flow charts or narrative descriptions.
- C) Walk throughs and limited system testing.
- D) Evaluate policy and procedures manuals the results from this review will have entailed.

Results of Internal Control Review

- Identification of the controls that the auditor will rely on during detailed testing.
- Description of the controls.
- Analysis of the controls.
- Evaluation of the appropriateness of the controls Risk Assessment.

It is important to consider other factors that may influence the assessment of the controls:

Other Influences on Controls

- Accidental or deliberate avoidance.

Training Material on Internal Audit

- Management override.
- Non-operation.
- Backup and recovery.
- Environmental impact.
- Formality.
- Means of communication.
- Access control over computer systems.

A re-analysis of risk and budget time will need to be done at this stage. The audit area may need to be prioritized lower/higher in the audit plan, or the amount of detailed testing may be revised.

Step 7. Detailed testing

To carry out sufficient audit tests of compliance and substantiation to gain sufficient evidence on the objective of the audit. Create or modify the audit programme based on risk findings established in the internal control review and information gathered in previous steps. The testing is aimed at significant controls that have previously been assessed as adequate to evaluate their effectiveness, and those controls assessed as inadequate to verify that the required results are not being consistently achieved.

Some verification techniques used may be:

- Observation and enquiry.
- Confirmation.
- Transaction testing.
- Analysis and Comparison.

It is important to accurately assess the **CAUSE AND EFFECT** of findings, and not to make assumptions.

Step 8. Draft the Report

The report has three purposes:

1. *Inform* - Clearly identify the difficulties or opportunities for improvement
2. *Persuade* - Using support for conclusions, and evidence of their importance
3. *Results* - Giving constructive and practical means of achieving the change

Step 9. Follow-Up

To ascertain that appropriate action is taken on reported audit findings, or that management of the board has assumed the risk of not taking correct action.

Illustrative Checklist for Production and Operations

Sr. No.	Control Parameters
	Operations
1	Machine and Tool Master List prepared and updated
2	Value of obsolete tool spares etc are documented and updated
3	Machine and Tools Down time are monitored and reviewed
4	Capacity utilisation for machines are monitored and reviewed
5	Production planning and scheduling is done at frequent intervals by a dedicated official keeping in perspective, the inventory position, the sales schedule and on-time

Sr. No.	Control Parameters
	delivery to customers.
6	Machine performance and output is monitored continuously
7	Continuous control is ensured for material rejection, in-process and customer reactions
8	Monitoring of budgeted vs. actual production is carried out and analysis of variance with reasons thereof, is documented.
9	Conservation of energy measures for lights, equipments, generators etc are implemented.
10	KPIs like Line utilisation rate, Overall Equipment Efficiency rates are monitored and abnormal fluctuations, if any are analyzed.

Illustrative Check-list : Materials Management and Issue to Production

Sr. No.	Control Parameters
	Stores and Inventory Management
	<i>Material Receipt System</i>
1	Material is accepted only against Purchase Orders.
2	Material is accepted only after the requisite Quality Inspection/tests are carried out.

Sr. No.	Control Parameters
3	Monitoring over time lag in receipt of the material vis-à-vis its inspection by the QC department is done on regular basis and/or report of the timelag is generated from the System to assess abnormal timelag and reasonwise analysis for remedial action plans.
4	Daily monitoring over rejected material to be sent back to the vendors after the 'hold period' is over.
5	Receipt notes are prepared for all materials received
6	Receipts are promptly recorded in Bin card and Bin card details are regularly updated
7	System of reporting shortage, rejection, non-receipt of consignment to purchase / accounts department
	<i>Stacking Arrangements</i>
8	Stacking norms for storage of material is defined and periodically reviewed for compliance.
9	Location earmarked and displayed for storage of various materials
10	Items are stored separately
11	Location of materials is easily identifiable from book records.
12	Separate location is specified for storage of rejected materials
	<i>Safety and Protection</i>
13	Adequacy of insurance coverage.

Sr. No.	Control Parameters
14	Custody of raw material is restricted to authorized persons of the Stores department and high value /dangerous inventory items are identified for their adequate security arrangements.
	<i>Physical stock-take</i>
15	Reconciliation of item-wise bookstock vis-à-vis physical stock is done and reasons for the difference identified
16	Segregation of the responsibilities for custody /accounting of stocks and reconciliation of physical stock vis-à-vis book stock is ensured.
	<i>Material Issue System</i>
17	Strict adherence to FIFO basis
18	Issue of material is only against specific system generated Materials Requisition and Issue Slip (MRS)/Jobcard/Batch to facilitate calculation of yield , wastage etc.
19	Authority for approval of MRS is defined and material is issued only against authorized MRS.
20	Instant recording of issued notes items to Bin card.
21	Acknowledgement of the receiving department is obtained on the MRS for the material issued.
	<i>Inventory Management</i>
22	SOP for perpetual stock-take is framed including schedule of perpetual inventory stock take, by classification of inventory items under ABC categories and monitored for compliances.

Sr. No.	Control Parameters
23	Periodic reports of non-moving/slow-moving stocks are generated and monitored regularly
24	Reconciliation of book-stock vis-à-vis physical stock is done and reasons for the difference identified.
25	Periodic inspection and verification of the raw material, is done to ensure that they do not get deteriorated / damaged
26	Verification of all incoming material is done by the gate security personnel and gate-in-stamp is put on all inward documents.
27	Measures are taken to ensure that inventory items are not left in the open under exposure of heat, rain etc.
28	Gate entry security procedures, controls and documentation in registers etc. enforced and reviewed for inbound and outbound materials and movement of personnel, visitors and workers
29	Ageing schedule of gate entry and GRNs made - % of GRN made on the day of gate entry
30	Frequent reconciliation of stores data and third party processor accounts (if applicable) done and reviewed

Checklist – Quality Control of Production

Sr. No.	Control Parameters
	Material Receipt System

Sr. No.	Control Parameters
	QA Controls
1	Material is accepted only after the requisite Quality Inspection/tests are carried out for steel strips and other items.
2	Inspection is carried out as per prescribed coverage of different categories of materials
3	Monitoring over time lag in receipt of the material vis-à-vis its inspection by the QC department is done on regular basis and/or report of the timelag is generated from the System to assess abnormal timelag and reasonwise analysis for remedial action plans.
4	Feedback on negative inspection results to purchase department
5	Procedure to conduct inspection at supplier site exists
6	Daily monitoring over rejected material to be sent back to the vendors after the 'hold period' is over.
7	Acceptance of material with deviation for quantity/ quality has been approved by competent authority
8	Lab testing equipments, consumables and equipment calibrations are monitored and adequate control measures are maintained
	Process Rejections
9	Joint certifications is done for process rejections to determine allowable rejections
10	Rework analysis % is monitored and corrective action taken with adequate documentation

Checklist- Health, Production Safety and Environment

Sr. No.	Control Parameters
	<i>She</i>
1	Plant safety is monitored and ensured
2	Adequate safety training and drills are conducted regularly to employees and contract workers
3	There is a structured Safety Policy / Standard which is understood and implemented at shop floor.
4	System is in place to monitor the employees and workers at shop floor whether they wear Plant Protective Equipments (PPE) like goggles, gloves, guards, helmets, ear plugs etc
5	Accidents are documented, analysed as to types, reasons and corrective / remedial action taken.
6	Adequate stock of safety equipments are maintained.
7	Periodic Safety Audit is carried out in line with OHSAS and ISO 140001 Mandates.

General Inspection Audit Check-points – Production / Shop-floor

General Controls – Electrical, Fire and Safety

Building _____

Engg. Plant____

Inspection performed by _____

Maintenance in-charge_____

Date _____

	Yes	No	Partial	COMMENTS
A. Walking Surfaces				
1. Aisles are established and are kept clear (minimum 36")				
2. No tripping hazards present				
3. Floors are even (no holes or cracks)				
4. Carpets, rugs, and mats do not present a tripping hazard				
5. Floors are kept dry as practical				
6. Entrance mats are available for wet weather				

Internal Audit of Production and Operations

	Yes	No	Partial	COMMENTS
7. Outside walkways and stairs are in good repair				
B. Electrical Hazards				
1. Extension cords are not used as permanent wiring and/or are unplugged from wall outlet when not in use				
2. When used, all extension cords are 3-wire type and in good condition - no splices or broken insulation are allowed				
3. If used, multi-outlet power strips are UL listed and have circuit breakers				
4. Extension cords and power strips are plugged directly into wall outlet, not other extension cords or power strips				
5. Equipment power cords are in good condition with no splices or broken insulation				
6. Plugs are in good condition - there are no exposed wires and the ground is not removed from 3-way plugs				

Training Material on Internal Audit

	Yes	No	Partial	COMMENTS
7. All wall outlet and junction box covers are in place				
8. Electric circuit panels are kept clear (at least 36 inches open area)				
9. Electrical circuits are not overloaded				
10. Wires or extension cords do not run under carpets or rugs, through doorways, or placed in other traffic areas				
C. Stairways, Ramps, Corridors, Storage Areas				
1. Lighting is adequate (including emergency lighting)				
2. Ramps have non-slip surfaces				
3. Stair treading is in good condition				
4. Stairways are kept clear and are not used for storage				
5. Handrails are in good condition				
6. Guardrails are installed (where needed)				

Internal Audit of Production and Operations

	Yes	No	Partial	COMMENTS
7. Corridors are kept clear of equipment and supplies				
8. No storage is allowed within 18 inches of sprinkler heads (24 inches of ceiling where no sprinkler system exists)				
9. Appropriate ladders are provided for high storage area access				
D. Office Equipment				
1. Step stools are available for use, where needed				
2. Oscillating fans have guards that prevent fingers from contacting fan blades				
E. Fire Prevention, Emergency Exits, Housekeeping				
1. Fire extinguishers are not obstructed				
2. Fire doors are not blocked open				
3. Exits are unobstructed and kept unlocked during normal business hours or special events				

Training Material on Internal Audit

	Yes	No	Partial	COMMENTS
4. Exits properly marked, exit signs illuminated				
5. Good housekeeping is practiced - liquid spills are absorbed, (especially oils), and excess paper and trash is removed				
6. Flammable/Combustible liquids are stored properly				
7. Electric space heaters are listed with working temperature controls and tip switches				
8. There are no holes through walls or ceilings, and all ceiling tiles are in place				
9. Occupancy limits are observed				

Checklist for Production and Operations Maintenance

Sr. No.	Control Parameters
	<i>Machine and Tool Maintenance</i>
1	Preventive Maintenance Schedule for each machine are prepared and maintenance carried out as per plan
2	Variance of Planned and Actual break downs, Machine Down time, Machine Shut Down and MTTR/ MTBF are monitored, documented and reviewed for corrective action
	<i>IT Maintenance</i>
3	Smoke detection and automatic fire extinguishing equipments installed to ensure that it is functional and that it provides adequate protection.
4	Potential threat posed by fires in adjacent buildings and areas are evaluated and adequate fire fighting equipments installed.
5	Alarms installed at all potential entry and exit points of sensitive areas

Internal Audit of Marketing

Segregation of Duties

The order entry, credit, shipping, billing, collecting, credit memo, MIS and general accounting activities need to be appropriately segregated if all control objectives are to be met. For example, those who perform the order entry (sales) activity, including those who maintain contact with customers and issue sales orders, would not perform any credit approval, shipping, billing, cash receipts, credit memo or accounting activities.

Key Aspects of Internal Audit of Marketing

- Business plan written
- Market analyzed
- Target market identified
- Industry analysis completed
- Market segment and niche identified
- Company strengths, weaknesses, opportunities and potential threats have been analyzed
- Prospects and customers profiled
- Target prospects and customers identified
- Customer needs and wants analyzed
- Customer purchasing "influencers" identified
- Competitive information gathered and compared
- Terms and conditions
- Pricing

- Delivery and service
- Market objectives
- Product is properly positioned in the market
- Product life cycle analyzed
- Know how product is perceived in market
- Return on investment objective set
- Product breadth and depth determined
- Cost and pricing objectives established
- Unit cost(s) analyzed and known
- Price elasticity analyzed
- Pricing strategies determined
- Promotional tools identified (discounts, allowances, freight, etc.)
- Risk analysis performed
- Specific business risks determined
- Environmental risks identified
- Economic risks analyzed
- Plan and budget established for marketing communications
- Communication objectives for target market
- Tracking and evaluation criteria established
- Sales Promotion
- Objectives and strategy
- Sales literature

Training Material on Internal Audit

- Differentiation theme/implementation objective
- Advertising and public relations
- Salient features and benefits established for target audiences(s)
- Media mix strategy determined
- Image of company is consistent and creative
- Trade show(s) share and illustrate the plan
- Customer service policies/plan established
- Periodically evaluated to meet customer needs
- Sales Plan
- Sales Forecasting Plan/Technique established
- Reps develop "ground-up" forecast with key customers
- Sales data captured and automation implemented
- Measurement and evaluation process in place
- Sales Management strategies and objectives
- Sales goal(s) and action plan per key customer written
- Top management understand stages of successful selling
- Sales channel(s) and distribution methods/ pricing evaluated
- Competitive comparison matrix
- Strategy for penetrating new markets

Illustrative Checklist

Sr. No.	Control Parameters
	<i>Sales and Accounts Receivables</i>
1	Record of Sales Orders (SO) received is maintained for all orders received from the customers and cross-verification of the orders received vis-à-vis orders entered in the System is done
2	Customer order check-list is maintained for all customers
3	Appropriate approval for further despatch of material to customers having over-due outstanding balances/sales order in excess of monetary credit limit.
4	Generation of a list of cancelled orders and orders not processed for each month along with the reasons for the same.
5	Timelag in receipt of order vis-à-vis actual despatch of goods analyzed and reasons for delays identified and corrective action initiated.
6	MIS of pending order is generated and reviewed periodically.
7	Fixation of monetary credit limits in order to control overdue balance vis-à-vis further despatches. System of Credit and / or Delivery Block is in place
8	Access to modify the blacklisting option of customers for executing sales restricted to authorized persons as per segregation of duties.
9	Access to generated sales invoice restricted to authorized persons.
10	Periodic MIS for sales return prepared and analyzed and corrective action initiated.

Sr. No.	Control Parameters
11	LC is cross checked with respect to LC check-list before issue of dispatch order to logistics department
12	Customer meets, Customer Satisfaction Surveys (CSS) are periodically initiated to develop market intelligence and obtain customer feedback on quality, delivery and pricing issues

Marketing KPI:

$$\begin{array}{l} \text{Customers Drop – out} \\ \text{or} \\ \text{Increase ratio} \end{array} = \frac{\left[\begin{array}{c} \text{No. of Active} \\ \text{Customers at} \\ \text{the being of} \\ \text{Period} \end{array} \right] + \left[\begin{array}{c} \text{No. of New} \\ \text{Customers} \\ \text{during the} \\ \text{period} \end{array} \right] - \left[\begin{array}{c} \text{No. of active} \\ \text{Customers at} \\ \text{the end of} \\ \text{period} \end{array} \right]}{\text{Number of active customers at the end of the period}}$$

Chapter-VI.3

Internal Audit of Finance and Accounts

Segregation of Duties

The handling of cash receipts and accounting for such receipts need to be segregated if all the control objectives are to be met. Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will remain undetected by providing an accounting check over the receipt of cash. For example, those who handle cash receipts would not have the authority to prepare or sign cheques, would not have access to accounting records, and would not be involved in reconciling bank accounts.

Key Control issues –

1. Personnel policies and active procedures are consistent.
2. Supervision of staff is adequate and in the auditor's opinion effective.
3. Administrative policies and active procedures are consistent.
4. Accounting policies and active procedures are consistent.
5. In the auditor's opinion, the internal controls are effective.
6. Expenses, costs and income are traceable and reasonable.
7. Daily and weekly cash reconciliation and records-keeping is consistent.
8. Communication between management and staff is in the auditor's opinion effective.
9. Cash and fixed assets are protected.

Checklists for Finance and Accounts

Sr. No.	Control Parameters
	<i>Finance and Accounts</i>
1	Management adopts accounting policies that best reflect the economic realities of the business.
2	Management has established procedures to prevent unauthorized access to, or destruction of, documents, records, and assets.
3	Incompatible duties are segregated (e.g., separation of accounting for and access to assets).
	<i>Cash and Bank Transactions</i>
4	Transactions are not accessible for any change of data entries without prior approval.
5	Pre-numbered receipt is in use as a token of acknowledgement of amount received from third parties/staff members. Delegation of power vested for approval of payment.
6	Vouchers are marked with "PAID" stamp to avoid any duplicate payments on the same set of document.
7	Frequency of cancellation of cheques are minimum.
8	BRS is prepared on a monthly basis
9	Minimum level of cash holding is maintained
10	System periodically validates that the financial system blocks a journal entry if the journal entry does not balance
11	System periodically validates that closing journal entries are blocked from being entered into the books for previous periods. Previous periods in the financial system should be locked to prevent changes

Sr. No.	Control Parameters
12	Perform reconciliation between bank statement and G/L for all cash accounts
13	Review outstanding checklist for any long outstanding checks. Determine resolution
	<i>Job Work (JW)</i>
14	DN raised against JW for process rejections
15	Control and review of Quantity and rates at which scrap lying at JW locations are sold.
16	System of sale of such scrap at JW locations at generation point and not brought back to factory to save transport costs
	<i>Insurance Coverage</i>
17	Review of adequacy of insurance coverage and premium payment for plant equipments, stock and accidental insurance , embezzlement/ damage etc.
18	Safe custody of insurance documents
19	System of Group Insurance Policy for employees, contract workers etc.
	<i>Cost Sheet Updation and Review</i>
20	System of Cost Sheet updation for product costing and adherence to budgeted cost, reviews of variances there on
	<i>Scrap Generation</i>
21	Analysis of standard and actual scrap generation is conducted periodically and corrective action taken.

Sr. No.	Control Parameters
	<i>Credit Management</i>
22	Following schedules/ MIS are periodically prepared and updated to ensure control of customer credit limits and recoverability followed by corrective action:
	a.) Customers exceeding credit limits. – customer, outstanding A/R, credit limit, over, reason, amount of over extension, reason thereof, overall customer credit rating
	b.) Customers extended credit despite having past due accounts. – customer, amount of earliest past due account, due date, amount of additional credit extended, reason
	c.) Statement of Account Dates – customer, cut-off date, date prepared, date received by customer
	d.) Customers extended credit without written approval. – customer, ref. inv., date, amount, reason.
	e.) Customers with expired credit agreements. – customer, credit limit, credit term, A/R , amount, reason thereof
	f) Officials extending credits beyond limits of authority – customer, inv. no., amount of credit, limit, concerned Sales / Marketing officer
	g) Report on legal cases
23	Reconciliation of customer balance is made frequently and completed within time frame

Checklists for Fixed Assets Management

Sr. No.	Control Parameters
	<i>Fixed Assets</i>
1	Periodic review of Fixed Assets Register (FAR) vis-à-vis monthly status of capital expenditure is done to ensure timely and accurate updation of FAR.
2	Fixed Assets Identification number is put all the assets and cross-verified with the FAR.
3	Physical verification of fixed assets is done at periodic intervals, as per the Fixed Assets Register (FAR) and results are documented.
4	Non-performing assets are periodically identified and documented and action plan for its disposal/alternate use initiated. Impairment testing carried out (AS 28) at each Balance Sheet date

Chapter-VI.4

Internal Audit of Human Resources

Segregation of duties

Timekeeping, handling the payroll cash disbursements, MIS, and accounting for payroll need to be appropriately segregated if all the control objectives are to be met. Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will remain undetected by providing an accounting check over the payment of salaries and wages.

Sr. No.	Control Parameters
	Payroll, Human Resource Management and Reporting
1	Management establishes and enforces standards for hiring the most qualified individuals for plant/ site operations, with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior.
2	Screening procedures, including background checks, are employed for job applicants, particularly for employees with access to assets susceptible to misappropriation in the plant.
3	Recruiting practices include formal, in-depth employment interviews and informative, insightful presentations on the entity's history, culture, and operating style.
4	Training policies communicate prospective roles and responsibilities and illustrate expected levels of performance and behavior.

Sr. No.	Control Parameters
5	Job performance is periodically appraised, evaluated and reviewed with each employee.
6	Disciplinary actions send a message that violations of expected behavior will not be tolerated.
7	An ongoing workshop and training programs, both on and off the job enables employees to deal effectively with various technical and administrative issues relating to plant operations, safety, machine maintenance, asset safeguarding and related areas.
8	There is a structure for assigning ownership of information including who is authorized to initiate or change transactions.
9	Employees throughout the entity are assigned authority and responsibility related to their specific job functions.
10	Job descriptions contain specific references to control-related responsibilities.
11	Employees are empowered, when appropriate, to correct problems or implement improvements.
12	Responsibility and delegation of authority are assigned to deal with organizational goals and objectives, operating functions, and regulatory requirements, including information systems and authorization for changes.
13	The entity establishes appropriate lines of reporting, giving consideration to its size and the nature of its activities.
14	Executives clearly understand their responsibility and authority for business activities and how they relate to the entity as a whole. Executives should possess the

Sr. No.	Control Parameters
	requisite experience and levels of knowledge to properly execute their positions.
16	Senior management maintains contact with and consistently emphasizes appropriate behavior to operating personnel.
17	The compensation committee approves all management incentive plans tied to performance.
18	Employees clearly understand what behavior is acceptable and unacceptable under the company's code of conduct and know what to do when they encounter improper behavior.
19	The importance of high ethics and internal controls is discussed with newly hired employees through orientations or interviews.
20	Management removes or reduces incentives or temptations that might cause personnel to engage in dishonest or unethical acts.
21	Management monitors departures from approved policies and procedures or violations of the code of conduct and takes appropriate disciplinary action.

A detailed sample check-list

Human Resources (Payroll and Disbursements) Audit

Objectives and Procedures

Overall Objective

To ensure that proper controls, policies and procedures are in place for each of the outlined areas below, and that records,

disclosures, and other information are consistent with plan documents and in compliance with applicable laws and regulation.

Preliminary Steps

1. Send a pre-audit/intro memo and hold a meeting with the main auditees.
2. Complete a preaudit review of accounts, previous audit concerns, examination and external findings, board minutes, fraud files, etc.
3. Obtain and evaluate strategic and incentive goals for the area, if any.
4. Interview unit management to determine if there were any significant losses attributed to employee error or possible fraud. Document each incident, including the final action against the employee, and the filing of any police reports,. Adjust audit tests as necessary
5. Complete a Lead Sheet listing accounts to be considered for review.
6. Estimate the time period and number of hours for completion.
7. Submit the results of these steps to the Head of Audit / Partner for review.

Objective A--Incentive Programs

Determine that incentive programs are properly documented, approved and communicated, established targets and levels are appropriate, and reported results and payouts are accurate.

Control Considerations

1. Incentive programs are formally documented and have been approved by the proper board committee and/or executive management.
2. Incentives are part of an overall documented compensation strategy for the positions involved.

Training Material on Internal Audit

3. Incentive programs are properly disclosed and communicated to all eligible employees.
4. Individual goals are appropriately linked to unit and overall organizational performance goals.
5. Management analyzes the success of the incentive programs by quantitative and qualitative analysis, and reports the results of the analysis to the board committee and/or executive management.
6. Results, incentives and rewards are accurately calculated and reported.
7. Incentive programs conform with regulatory requirements.

Procedures

1. Obtain written documentation on all incentive plans. Review goals and targets. Check if they have been properly reviewed and approved.
2. Review management's analysis of the program's effectiveness in rewarding performance toward individual and organizational sales goals.
3. Document processes and controls involved in tracking, tabulating, reporting, and paying for results for the program.
4. Perform analytical review of aggregate incentive totals. Calculate % of payout to base wages. Compare individual incentives as a % of base wages for a sample of employees. Compare to program goals.
5. Obtain individual calculations of results for selected periods. Trace back to proof of sales. Determine accuracy of reported results.
6. Recalculate incentives and compare to reported amounts. Trace reported amounts to actual payroll posting.

7. Determine that the plans are properly structured and monitored in compliance with applicable rules and regulations.
8. Conclude on the objective.

Objective B--Employee Bonus Program

Determine that the employee bonus program is properly documented, approved and communicated, established targets and levels are appropriate, and reported results and payouts are accurate.

Control Considerations

1. The bonus program is formally documented and has been approved by the proper board committee and/or executive management.
2. Plan goals are appropriately linked to the overall organizational performance goals.
3. The bonus program is properly disclosed and communicated to all eligible employees.
4. Bonuses are accurately calculated, reported and paid.

Procedures

1. Obtain written documentation on the bonus program. Review goals and targets and compare to entity's strategic goals. Determine that the program has been properly reviewed and communicated.
2. Document processes and controls involved in tracking, computing reporting, and paying bonuses.
3. Perform analytical review of performance against program targets. Determine whether or not a bonus should have been paid for each applicable quarter.
4. Recalculate bonus percentages. Determine eligible employees for selected payout quarters, and trace to proper calculation and payroll payment.
5. Conclude on the objective.

Objective C--Executive Bonus Program

Determine that the executive bonus program is properly documented, approved and communicated, established targets and levels are appropriate, and reported results and payouts are accurate.

Control Considerations

1. The executive bonus program is formally documented and has been approved by the executive committee of the board.
2. Plan goals are appropriately linked to the overall organizational performance goals.
3. The bonus program is properly disclosed and communicated to all eligible employees.
4. Bonuses are accurately calculated, reported and paid.

Procedures

1. Obtain written documentation on the bonus program. Review goals and targets and compare to entity's strategic goals. Determine that the program has been properly reviewed and approved.
2. Document processes and controls involved in tracking, computing reporting, and paying bonuses.
3. Perform analytical review of performance against program targets. Determine whether or not a bonus should have been paid for each applicable period.
4. Recalculate expected bonus percentages based on plan documentation. Obtain confirmation that bonuses paid were accurate based on this calculation.
5. Conclude on the objective.

Objective D--Pension Plan

Determine that the benefits accrued, earned and paid under the plan are estimated, calculated, communicated, and paid on an accurate and timely basis. Also, determine that the records of the trustee accurately reflect the aggregate of participant asset balances, earnings and transaction activity.

Control Considerations

1. The plan is properly documented and communicated to all employees at date of hire, date of eligibility, and at other periods as appropriate or required.
2. Plan information is constantly updated and made available to employees via the corporate intranet and other delivery methods.
3. Accurate, individual estimates are made available to employees on a confidential and timely basis.
4. Tools are provided via the corporate internet or other delivery methods to allow employees to reasonably calculate future estimated plan benefits.
5. All eligible employees are included in the plan on a timely basis.
6. Annual census and payroll information is accurately reported to the plan actuary.
7. Benefit payments are calculated accurately and paid timely.
8. Balances per the trustee statements are reasonable based on investment activity, contribution activity, investment gains and losses, and plan expenses.
9. Investment allocations and activity are within the established investment policy's guidelines.
10. Investment income and unrecognized gains/losses are reasonable.

Training Material on Internal Audit

11. Contributions are properly and timely recognized by the trustee.
12. Aggregate participant payout information is accurately reflected in the trustee's records.
13. Overall plan costs and investment returns are analyzed by management and/or the appropriate board committee.
14. Pension cost is properly recognized in the financial statements
15. Transition to new providers of investments services and recordkeeping/actuary services, if any, was done appropriately, timely and accurately.

Procedures

1. Review the plan document. Note key provisions for participation, benefit determination, vesting and withdrawal. Discuss with HR staff and review pension committee minutes for any plan changes since the last audit.
2. Determine whether any changes were made to investment managers or actuaries/recordkeepers during the audit period. Briefly document the research, selection, approval and communication processes.
3. Review employee policies and communications relating to the plan. Assess the quality, accuracy and understandability of the information.
4. Document the processes for enrollment and processing terminations.
5. Pull information from the HR system to test new employees and newly eligible employees for inclusion in the plan. Test accuracy of reported information against actuary reports.
6. Pull information from the HR system to test for employee terminations. Review actuary documents and trace to trustee records for evidence of accurate disbursement directly to credit of the participant.

7. Recompute a sample of benefits paid for accuracy of calculation based on participant data and plan provisions.
8. Review a sample of individual employee estimates for the last two years. Verify the amounts and percentages used and recalculate the estimated benefits.
9. Obtain a trustee listing of participant payouts. Trace to evidence of termination.
10. Obtain trustee statements for the audit period. Schedule activity and review for reasonableness.
11. Determine cash contributions during the audit period. Trace to trustee statements and approval by committee or board.
12. Review administrative expenses paid per the trustee statement. Compare to amounts per entity financial statements. Determine appropriateness per contract.
13. Obtain annual benefit plan statements from the actuary. Determine that benefit costs are properly recognized in entity financial statements.
14. Review management's or the board committee's analysis of the performance of the actuary and trustee.
15. Trace balances from prior to current providers. Determine that balances were transferred accurately, timely and at the proper value.
16. Conclude on the objective.

Objective E

Determine that employee and company contributions, earnings, loans, withdrawals and payouts are accounted for accurately and timely.

Also, determine that the records of the trustee accurately reflect the aggregate of participant asset balances, earnings and transaction activity.

Control Considerations

1. The plan is properly documented and communicated to all employees at date of hire, date of eligibility, and at other periods as appropriate or required.
2. Plan information is constantly updated and made available to employees via the corporate intranet, provider website and materials, periodic meetings, etc.
3. Participants receive quarterly statements on a timely basis that accurately show their investment allocations, balances, activity and contributions.
4. Tools are provided via the internet or other delivery methods to allow employees to reasonably calculate future estimated benefits.
5. Newly eligible employees receive timely information on their ability to participate in the plan.
6. Open enrollments periods are maintained in compliance with the plan document.
7. Periodic enrollment meetings are held to communicate the benefits of the plan to potential and current participants.
8. Adequate information is provided on investment options to allow employees to make informed choices as required by regulation.
9. Only licensed representatives provide investment advice to participants.
10. Company matches are calculated and posted accurately and timely.
11. Loans and hardship withdrawals are administered in accordance with the plan document.
12. Plan terminations are paid accurately and timely.

Internal Audit of Human Resources

13. Balances per the trustee statements are reasonable based on investment activity, contribution activity, investment gains and losses, and plan expenses.
14. Investment allocations are made accurately and timely to participant accounts.
15. Investment income and unrecognized gains/losses are reasonable.
16. Participant contributions are properly segregated and allocated.
17. Aggregate participant payout information is accurately reflected in the trustee's records.
18. Plan costs and contributions are properly recognized in entity's financial Statements.
19. Overall plan costs and investment returns are analyzed by management and/or the appropriate board committee.
20. Transition to new providers of investments services and recordkeeping, if any, was done appropriately, timely and accurately.

Procedures

1. Review the plan document. Note key provisions for participation, benefit determination, vesting and withdrawal. Discuss with HR staff and review pension committee minutes for any plan changes since the last audit.
2. Determine whether any changes were made to investment managers or recordkeepers during the audit period. Briefly document the research, selection, approval and communication processes.
3. Review employee policies and communications relating to the plan. Assess the quality, accuracy and understandability of the information.

Training Material on Internal Audit

4. Pull information from the HR system to determine that newly eligible and eligible non-participants are informed timely of their option to participate.
5. Document the process for processing loans, terminations, and paying benefits.
6. Pull information from the HR system to test for employee terminations. Trace to trustee records for evidence of accurate disbursement directly to the credit of the participant.
7. Review loan disbursements. Trace to receipt by the participant. Determine that loan terms conform to the plan document.
8. Trace payments to canceled checks on a test basis and compare endorsements to signatures on file, if applicable.
9. Obtain trustee statements for the audit period. Schedule activity and review for reasonableness.
10. Obtain a trustee listing of participant payouts. Trace to loan agreements or evidence of termination.
11. Determine total contributions made by the entity during the audit period. Trace to trustee statements.
12. Review administrative expenses paid per the trustee statement. Compare to amounts per entity financial statements. Determine appropriateness per contract.
13. Review management's or the board committee's analysis of the performance of the actuary and trustee and compare to the investment policy standards.
14. Trace balances from prior to current providers. Determine that balances were transferred accurately, timely and at the proper value.
15. Conclude on the objective.

Chapter-VI.5

Internal Audit of Information Technology

Organization and Administration of EDP/ IT Department – General Queries of Internal Auditor

1. Is there a separate EDP department within the Company?
2. Is there a steering committee and their duties and responsibilities for managing MIS are clearly defined?
3. Has the Company developed an IT strategy linked with the long and medium term plans?
4. Is the EDP Department independent of the user department and in particular the accounting department?
5. Are there written job descriptions for all jobs within EDP department and these job descriptions are communicated to designated employees?
6. Are EDP personnel prohibited from having incompatible responsibilities or duties in user departments and vice versa?
7. Are there written specifications for all jobs in the EDP Department?
8. Are the following functions within the EDP Department performed by separate sections:
 - System design.
 - Application programming.
 - Computer operations.
 - Database administration.
 - Systems programming.
 - Data entry and control?

Training Material on Internal Audit

9. Are the data processing personnel prohibited from duties relating to:
 - Initiating transactions?
 - Recording of transactions?
 - Master file changes?
 - Correction of errors?
10. Are all processing prescheduled and authorised by appropriate personnel?
11. Are there procedures to evaluate and establish who has access to the data in the database?
12. Are the EDP personnel adequately trained?
13. Are systems analysts programmers denied access to the computer room and limited in their operation of the computer?
14. Do any of the computer operators have programming knowledge?
15. Are operators barred from making changes to programs and from creating or amending data before, during, or after processing?
16. Is the custody of assets restricted to personnel outside the EDP department?
17. Is strategic data processing plan developed by the company for the achievement of long-term business plan?
18. Are there any key personnel within IT department whose absence can leave the company within limited expertise?
19. Are there any key personnel who are being over - relied?
20. Is EDP audit being carried by internal audit or an external consultant to ensure compliance of policies and controls established by management.

Illustrative Checklist for Internal Audit of IT systems

Sr. No.	Control Parameters
	IT Management
	<i>IT Access Control</i>
1	There is a structured IT Policy and facility personnel are aware of the applicable policies.
	<i>IT Back-up and Recovery</i>
2	The network has adequately documented backup and recovery procedures/plans/schedules for critical sites.
3	LAN is supported by an uninterruptible power supply (UPS).
4	UPS tested in the last year (to test the batteries)?
5	For disaster-recovery purposes, LAN applications have been prioritized and scheduled for recovery based on importance to the operation.
	<i>IT Environmental Controls</i>
6	Smoke detection and automatic fire-extinguishing equipments installed for adequate functioning and protection against fire hazards
	<i>IT Inventory</i>
7	There is a complete inventory of the following: Hardware: Computers, File Servers, Printers, Modems, Switches, Routers, Hubs, etc. Software: all software for each PC is logged with licenses and serial numbers.
8	There are written procedures for keeping LAN inventory. And they identify who (title) is responsible for maintaining the inventory report.

Sr. No.	Control Parameters
9	Unused equipment is properly and securely stored.
	<i>IT Operations</i>
10	LAN administrator has a backup person.
11	LAN administrator monitors the LAN response time, disk storage space, and LAN utilization.
12	LAN administrator is experienced and familiar with operation of the LAN facility.
	<i>IT Physical Security</i>
13	Alarms installed at all potential entry and exist points of sensitive areas.
	<i>IT Service Agreements</i>
14	Vendor reliability considered before purchasing LAN hardware and software.
15	Service log maintained to document vendor support servicing.
16	LAN hardware and software purchase contracts include statements regarding vendor support and licensing.
	<i>IT Virus Protection Policy</i>
17	The level of virus protection established on servers and workstations is determined and the monitoring of infection are being done by IT administration. Virus Application should be updated on a monthly basis. Laptops if issued should be ensured to have secured internet access.

Access Controls Audit Program (Illustrative)

Access Controls

I. Audit Program Overview

Access to computer resources should be controlled to protect them against unauthorized use, damage, loss, or modifications. Proper access controls will assist in the prevention or detection of deliberate or accidental errors

caused by improper use or manipulation of data files, unauthorized or incorrect use of computer programs, and/or improper use of computer resources.

Suggested interviewees for ICQ:

- A. Documentation Librarian.
- B. System Programming Manager.
- C. Applications Programming Manager.
- D. Director of Data Processing.
- E. Data Base Administrator.

II. Tests of Compliance

A. Control Objective #1 - Access to Program Documentation

1. Observe the storage location of documentation if it is kept in printed form or determine how access to on-line documentation is restricted. Determine if the documentation is adequately secured.
2. Review documentation check out logs to see if only authorized persons are gaining access to documentation. Determine if checked out documentation is properly logged and can be located.

B. Control Objective #2 - Access to Systems Software

1. Interview the person responsible for access to system software. Determine if the methods used to limit access to systems software to authorized persons are adequate.
2. Review documentation check out logs to see if only authorized persons are gaining access to documentation. Determine if checked out documentation is properly logged and if it can be located.
3. Test to see that access to systems software is limited by terminal address.

C. Control Objective #3 - Access to Production Programs

1. Interview the person responsible for controlling access to production programs (source and object code) and job control instruction. Determine if passwords and utilities that affect program access are adequately controlled. Also determine if controls are adequate to limit access to only those who need it in their jobs.

D. Control Objective #4 - Access to Data Files

1. Review the procedures for limiting access to data files. Determine if programs not in the production library are adequately restricted from processing against data files and if controls are adequate to restrict access to data files to only authorized persons.

E. Control Objective #5 - Access to On-Line Systems

1. Determine who has access to confidential data. Verify with the owner of the data that these persons have authorization to access this data.
2. Test to see that access to applications, data, or entry and update of transactions is limited by terminal address and hours of operation.

3. For employees that have requested that their addresses and phone numbers not be disclosed, determine if this information is adequately protected from disclosure.

F. Control Objective #6 - Access to Data Bases

1. Interview the data base administrator and determine if controls are adequate to restrict access to the data base and data base change utilities.
2. Determine how concurrent access to the same data item is prevented and if it is adequate.

G. Control Objective #7 – Password Administration

1. Review the procedures for controlling passwords and determine if they are complete.
2. Interview users to determine when passwords were last changed.
3. In a department where an employee has recently terminated, determine if the employee's password has been deleted and if the passwords of other employees in the department have been changed.
4. Determine how access to password tables is restricted. Determine if access is restricted to only those who really need to access the table.
5. Test to see that there is a limit on the number of unsuccessful attempts to sign on (or login).

H. Control Objective #8 - Policies for Access Security

1. Review the policies for access security. Determine if they are complete.
2. Interview the person(s) responsible for access security and determine if they are aware of and follow the policies for access security.
3. Review logs that record accesses. Compare the logs to the list of authorized persons. Determine if access violations are being investigated in accordance with procedures.

III. Effect of Weaknesses

Access controls are designed to limit access to documentation, files, and programs. A weaknesses in or lack of such controls increases the opportunity for unauthorized modification to files and programs, as well as misuse of the computer hardware. Weaknesses in documentation and/or controls over machine use may be compensated by other strong EDP controls. However, weaknesses in systems software, program, and data security significantly decrease the integrity of the system. Weaknesses in this area must be considered in the evaluation of application controls.

Sample Audit Program for Business Continuity Program / Disaster Recovery Program

Step	Task Description	Task Performed By	Est. Time	W/P Ref.
	<i>Tactical Alignment</i>			
BC1	Discuss the business' strategy with regard to Business Continuity planning. Determine if the strategy focuses on IT Disaster Recovery Planning, which may be limited to restoring IT infrastructure at an alternative location or if it has a more holistic business orientation focusing on resuming all critical business operations. Assess whether the strategy: <ul style="list-style-type: none">• Considers business drivers, vulnerabilities and impacts?			

Step	Task Description	Task Performed By	Est. Time	W/P Ref.
	<ul style="list-style-type: none"> • Prioritizes risks and recovery alternatives according to a Business Impact Analysis? • Addresses both IT and non-IT business processes and resources? • Has been formally defined, documented and communicated as a part of the goals of Business Continuity Management? 			
BC2	<p>Gather management's perception of the most critical business processes (and why), and management's formal/informal assessment of the effectiveness of the company's ability to resume business operations in the event of a disruption. Determine the basis for this evaluation (e.g., stakeholder feedback, experience during a previous outage).</p> <p>Discuss whether the existing Business Continuity Management Processes are adequately serving the organization's needs.</p>			

Step	Task Description	Task Performed By	Est. Time	W/P Ref.
	<i>Stability and Reliability</i>			
BC3	<p>Determine if the business risks and impacts of unexpected disruptions have been identified and quantified by management. In the discussion, determine whether:</p> <ul style="list-style-type: none"> • Critical applications and business processes have been identified. • Vulnerabilities and risks to critical resources have been identified. • A formal risk analysis has been performed. • Potential business impacts of disruptions have been identified. • The business is aware of what it will need to continue delivering business services. 			
BC4	<p>Review the analysis of the organization's previous business continuity tests. Determine if the tests were successful. If not, why not? Identify recurring issues or other potential problem areas and understand the reasons for their existence. Are there any areas of the business that were not presented in the plan or the test? If so, why?</p>			

Step	Task Description	Task Performed By	Est. Time	W/P Ref.
	<i>Processes</i>			
BC5	Review documentation the organization has developed regarding business continuity processes, policies, standards and service level agreements. Determine if the processes are adequately documented, maintained and communicated to appropriate personnel.			
BC6	<p>Determine if a Business Continuity Plan exists and assess the degree to which it has been defined, documented, tested, maintained and communicated. Consider the following:</p> <ul style="list-style-type: none"> • Does it address critical applications and processes? • Does it address back-up, recovery and alternative operating procedures? • Personnel requirements? • Does it address both IT service resumption as well as business operations resumption? • When was the last time it was tested? • When was the last time it was updated? 			

Step	Task Description	Task Performed By	Est. Time	W/P Ref.
	<ul style="list-style-type: none"> Who maintains the plan and how? How are requirements communicated both to and from the business units? 			
	<i>Technology Leverage</i>			
BC7	<p>Determine the degree to which the organization uses software tools to facilitate Business Continuity Management processes. For example:</p> <ul style="list-style-type: none"> Job flow analysis tools to identify all system components of a given business task. Systems and network management tools used to identify potential service interruptions and automatically notify key personnel. Automated tools for backup and recovery of critical resources. Document management tools to manage changes to the Business Continuity Plan. 			

Step	Task Description	Task Performed By	Est. Time	W/P Ref.
	<i>Results Management</i>			
BC8	Determine what Service Level Agreements are in place between the function chartered with Business Continuity Management, its various support organizations and other business units. Understand what the agreements include and discuss the criteria for determining SLA achievement. Have there been instances where this has or has not been achieved?			
BC9	Identify the process for testing the Business Continuity Plan. Determine if the frequency of testing is adequate. Do tests reflect a realistic set of scenarios? How are tests results evaluated, reported and used as input for continuous improvement?			
	<i>Human Capital</i>			
BC10	Determine if responsibility for the overall development, testing and maintenance of the Business Continuity Plan has been assigned to a particular individual or group. Discuss the group's responsibility for			

Training Material on Internal Audit

Step	Task Description	Task Performed By	Est. Time	W/P Ref.
	coordinating the planning, testing and execution of the Business Continuity Plan. Have the roles and responsibilities of the group been documented and communicated?			
BC11	Discuss the relationship between the group responsible for coordination of Business Continuity Management activities and the support of other business functions. Discuss how the various business functions interact to understand relationships between business processes and how they use this information to develop and maintain the Business Continuity Plan.			

Chapter-VI.6

Risk Templates, Risk Reporting

A. Audit Procedures

Audit Procedures	W.P.	Done	Time	Date	Date		Che- cked
	Ref.	By	Spent	Expe- cted	Fini- shed	Re- mar ks	By:
1. Obtain schedule of Receivables. Check footings and cross-footings. Trace amounts on schedule to subsidiary ledgers. 2. Trace postings on control accounts and subsidiary ledgers to source documents (invoices, PR's, JV's, etc.). Check accuracy of accounting entries. Investi- gate unusual transactions.							

B. Risk Analysis and Risk Assessment - Guidelines

Access Risk	Probability	Exposure
Access risk refers to the impact of unauthorized access to any company assets, such as customer information, passwords, computer hardware and software, confidential financial information, legal information, cash, checks, and other physical assets. When evaluating access risk the nature and relative value of the company's assets need to be considered.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Business Disruption Risk	Probability	Exposure
<p>Business disruption risk considers the impact if the function or activity was rendered inoperative due to a system failure, or a disaster situation. Consideration is given to the impact on Company customers as well as other Company operations.</p>	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Data Integrity Risk	Probability	Exposure
<p>Data integrity risk addresses the impact if inaccurate data is used to make inappropriate business or management decisions. This risk also addresses the impact if customer information such as account balances or transaction histories were incorrect, or if inaccurate data is used in payment to/from external entities. The release of inaccurate data outside the Company to customers, regulators, shareholders, the public, etc. could lead to a loss of business, possible legal action or public embarrassment.</p>	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Credit Risk	Probability	Exposure
Credit risk considers the potential that extensions of credit to customers may not be repaid. There is an element of credit risk in each extension of credit. When setting lending policies and procedures, the company must consider what level of credit risk is acceptable. Extension of credit includes the use of debit cards and credit cards by customers to make EFT purchases.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Customer Service Risk	Probability	Exposure
Customer service risk considers the likely impact on customers if a control should fail. A customer may be external or internal to the company. For example, the line units are customers of the support units. When the customer is internal, assessment of customer service risk should also consider how problems with internal services will likely impact the level of service offered to the outside customer.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Financial/External Report Misstatement Risk	Probability	Exposure
Financial/external report misstatement risk is similar to data integrity risk. However, this risk focuses specifically on the company's general ledger and the various external financial reports which are created from the G/L. Consideration of Generally Accepted Accounting Principles and regulatory accounting principles is an important factor in evaluating financial report misstatement. This risk includes the potential impact of negative comments on the external auditor's Notes to Financial Statements or Management Letter.	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low <input type="checkbox"/> N/A	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low <input type="checkbox"/> N/A

Float Risk	Probability	Exposure
Float risk considers the opportunity cost (lost revenues) if funds are not processed or invested in a timely manner. This risk also addresses the cost (additional expenses) if obligations are not met on a timely basis. Receivables, Payables and suspense accounts are subject to float risk.	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low <input type="checkbox"/> N/A	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low <input type="checkbox"/> N/A

Fraud Risk	Probability	Exposure
Both internal and external fraud risks need to be considered. Internally, employees may misappropriate company assets, or manipulate or destroy company records. Externally, customers and non-customers may perpetrate a fraud by tapping into communication lines, obtaining confidential company information, misdirecting inventories or assets, etc.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Legal And Regulatory Risk	Probability	Exposure
In evaluating legal and regulatory risk, consider whether the product, service, or function is subject to legal and regulatory requirements. regulatory requirements may be federal, state or local. The relative risk level of an objective may be high if the related law/regulation is currently on the most dangerous violation list. Legal risk also considers the likelihood of the company being sued under a civil action for breach of contract, negligence, misrepresentation, product liability, unsafe premises, etc.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Physical Harm Risk	Probability	Exposure
Physical harm risk considers the risk of harm to both employees and customers while in the Company premises or while performing company business. This risk also applies to company assets such as computers or other equipment which may be damaged due to misuse or improper set-up and storage, or negotiable instruments and other documents which may be damaged or destroyed.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Other Considerations	Probability	Exposure
Consider the impact of all other relevant factors on risk. Consider, for instance, the transaction volumes (items and dollars), and financial impact on the balance sheet and income statement.	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low
	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A

Overall Rating	Probability	Exposure	Overall Risk
Based on the evaluation of: What can go wrong ? (probability); and what is the cost if what can go wrong, does go wrong ? (the exposure); evaluate the overall magnitude of the risk in the area/function. Evaluate the Probability and Exposure, then combine the two for an estimate of Overall Risk of business mission failure.	<input type="checkbox"/> High	<input type="checkbox"/> High	<input type="checkbox"/> High
	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
	<input type="checkbox"/> Low	<input type="checkbox"/> Low	<input type="checkbox"/> Low

Risk and Audit Universe (Sample)

F – Risk and audit universe (part)


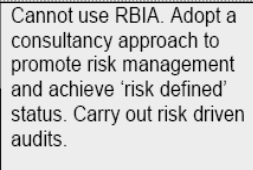
Key risk to process	Response	Control (examples)	Monitoring (examples)	Cous	Like	Score	Control score	Audit action	Next audit number	Next audit name	Next timing
the objective will not deliver the organisation's objectives effectively and effectively	treat	Overall targets for sales and profits are set by the board in the budget package the Merchising Director outlines the action to be taken to achieve the targets see case strategy controls	Monthly reports of sales and Profits are presented to the Board. with an explanation of variances	5	1	5	20	audit	200	selling strategy	jun-06
Fai to stok 90005 which the customers went to buy	treat	Regular visits by Merchising Director and staff to markets which anticipate at trade shows. focus Groups	Quarterly Presentation to Board by Merchising Director on Market trends	5	1	5	20	audit	2001	Market anticipation	jun-06
Fai to anticipate the competitors' intentions to take a bigger market share	treat	All competitors' advertising campaigns monitored with a weekly report to the Merchising Director	None	5	1	15	20	audit	2001	Market anticipation	jun-06
Prices are not Competitive Store layout confuses customers	treat	Competitors' prices are monitored every week, with Report going to appropriate Reading of Merchising Department	None	5	1	10	15	consultancy	2001	Market	Feb-06
	treat		None	5	1	16	15	consultancy	203	Store Planning	Mer-06
Prices are incorrect	treat	Retail prices are input by an assistant buyer and by an assistant buyer and checked by a supervisor prices are downloaded onto the EPOS system over night	A gross profit exception report is generated for any changes to Gp >5% This should pick up any incorrect input of retail Prices the reports is signed off by a buyer.	4	1	4	16	audit	204	Price file maintenance	Apr-06

Audit Conclusions (illustrative)

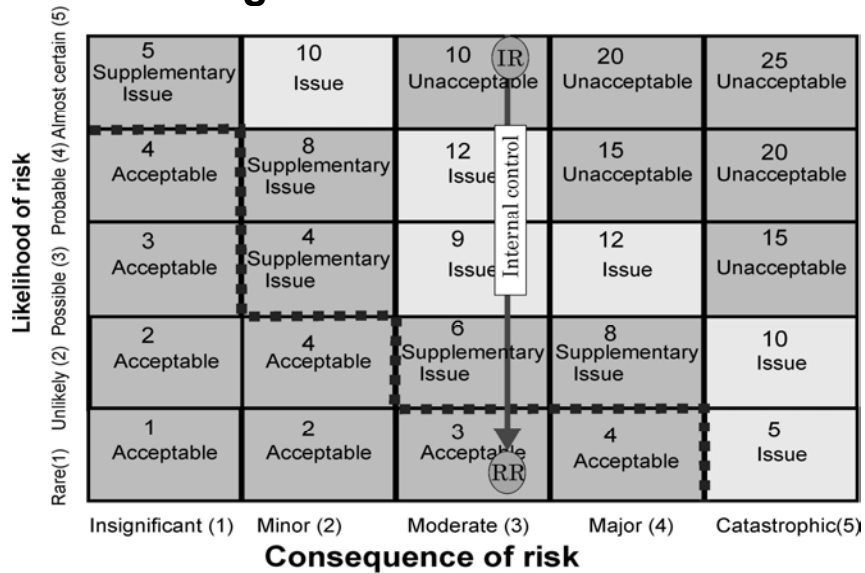
Guidance on assigning audit conclusions

Conclusion on:	Criteria		
Risk have been identified, evaluated and managed	Thorough processes have been used and all significant risk should have been identified	Processes have been used, but there are some deficiencies and not been identified.	Inadequate, or no, processes have been used.
Internal controls reduce risks to acceptable levels (that is to within the risk appetite of the organisation)	Risk are being managed to within acceptable levels, as defined by the board Report as Supplementary issue, if cost effective controls can reduce the risk further, otherwise do not report	Not all risk are being managed to within acceptable levels as defined by the board, although the consequence from the risk occurring, or likelihood of the risk occurring, is not considered significant there is the possibility that some objective will not be achieved Report as: Key issue	this risk is not being mitigated to an acceptable level by the control (s) and it is probable that some objective will not be achieved, with significant results Report as: Key issue No action is being taken
Action being taken to promptly remedy significant failings or weaknesses current levels of monitoring are	the action being taken will result in all risks being managed to within acceptable levels no more monitoring is necessary	the action being taken will result in some reduction in risk but not to acceptable levels Some additional monitoring is required	OR insufficient action is being taken to manage risks to within acceptable levels Major improvements are required to the monitoring of controls
Colour:	Green		
Grading:	Acceptable	Issues	Unacceptable

Risk, Controls and associated Audit Approach

	Controls	Monitoring	Audit approach
Risk enabled	All risks identified and assessed. Regular reviews of risks. Responses are in place to manage risks	Management monitor that all types of response are operating properly. All managers provide assurance on the effectiveness of their risk management and are assessed on their risk management performance	
Risk managed		Management monitor that all types of response are operating properly. Most managers provide assurance on the effectiveness of their risk management and are assessed on their risk management performance	
Risk defined	Majority of risks identified and assessed. Regular reviews of risks. Responses are in place to manage most risks	Some management monitoring that all types of response are operating properly	
Risk aware	Controls may be in place but are not linked to risks	Little monitoring	Cannot use RBIA. Adopt a consultancy approach to promote risk management and achieve 'risk defined' status. Carry out risk driven audits.
Risk naive	Controls, but some may be missing or incomplete	Very little, if any monitoring	

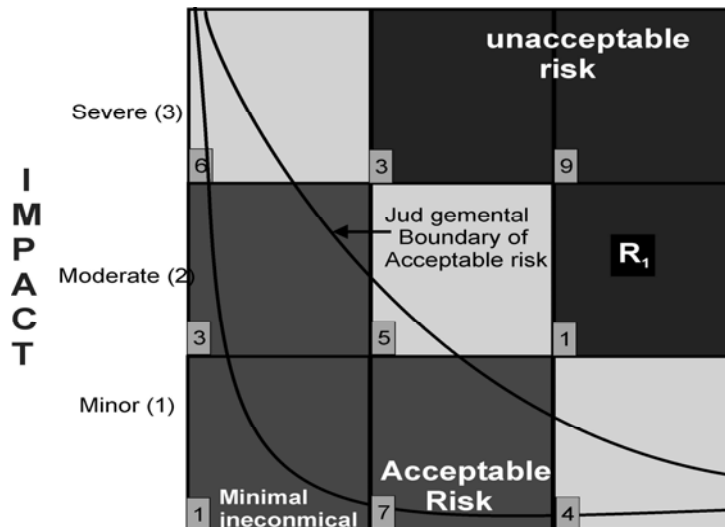
Risk scoring matrix



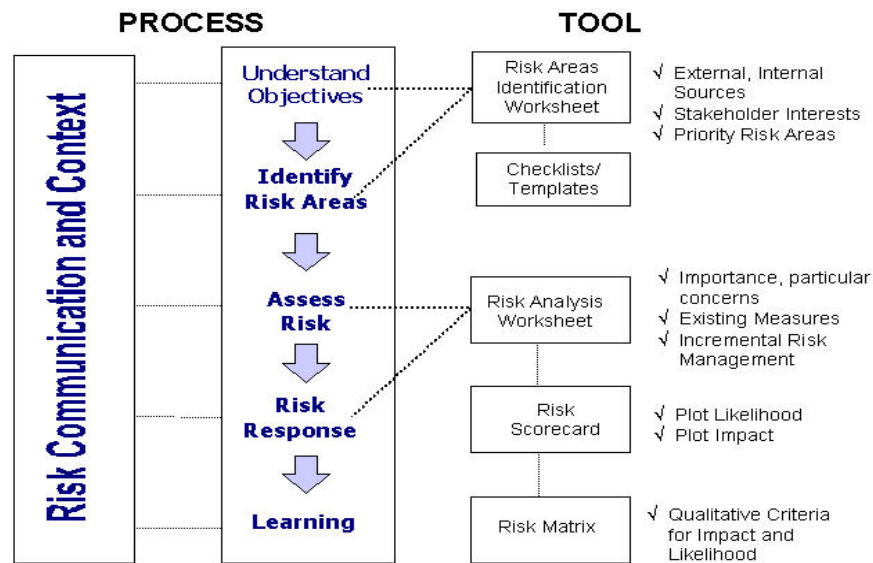
Unacceptable : Immediate action required manage the risk
Issue: Action required to manage the risk
Supplementary issue: Action is advisable if resources are available
Acceptable: No action required
 ■ ■ ■ ■ Risk appetite, as defined by the board

IR=Inherent Risk RR = Residual Risk

Risk – likelihood Impact matrix



Risk Communication



Risk Management Actions Template

Impact	Risk Management Actions		
Significant	Considerable management required	Must manage and monitor risks	Extensive management essential
Moderate	Risk may be worth accepting with monitoring	Management effort worthwhile	management effort required
Minor	Accept risk	Accept, but monitor risk	manage and monitor risks
	Low	Medium Likelihood	High

MODULE - VII

SPECIALISED INTERNAL AUDITS – DUE DILIGENCE; INVESTIGATION; FRAUD DETECTION; CONCURRENT AUDIT

Chapter-VII.1

Introduction on Due Diligence

The world has seen paradigm shift in the capital and trade which has resulted in the dramatic restructuring of companies in the form of amalgamations, acquisitions, mergers, and joint ventures has almost become a norm. New business structures through public-private partnerships, concession arrangements, etc. also have emerged. It is in this context that assessing the potential risks of a proposed transaction by inquiring into all relevant aspects of the past, present and predictable future of the business to be ventured has become quintessential. This exercise is referred to as 'Due Diligence'.

What is Due Diligence ?

Most legal definitions of due diligence describe it as a measure of prudence activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent person under the particular circumstance; not measured by any absolute standard but depends on the relative facts of the special case. In other words, making sure one gets what one thinks he/ she is paying for.

Why Such Due Diligence is Needed ?

When a business opportunity first arises, it continues throughout the talks, initial data collection and evaluation commence. Thorough detailed due diligence is typically conducted after the parties involved in a proposed transaction have agreed in principle that a deal should be pursued and after a preliminary understanding has been reached, but prior to the signing of a binding contract. There are many reasons for carrying out due diligence including:

- To confirm that the business is what it appears to be;
- To identify potential 'deal killer' defects in the target and avoid a bad business transaction;

- To gain information that will be useful for valuing assets, defining representations and warranties, and/or negotiating price concessions; and
- To verify that the transaction complies with investment or acquisition criteria.

Protecting Confidentiality of the Information

Due Diligence talks about the information hence required the flow of confidential. The Flow of confidential information based on the overall progress of the transaction is one of the best means of protection. In other words, less sensitive information should be shared initially, and as the potential buyer progresses and shows seriousness; more sensitive information could be shared. It forces the potential buyer to earn the more sensitive information and limits the number of parties who see the confidential records.

The phasing of information flow could follow the pattern mentioned below:

- The first phase consists of information that are already in public domain.
- The next phase consists of information that is typically heavier on current and historical matters than on forward-looking projections. Quite a bit of confidential company information is disclosed at this stage, but very little that is competitively sensitive.
- The third phase involves the most sensitive company information, including projections, customer information and any other information requested by the buyer deemed too sensitive to share earlier in the process.
- Finally, the accounting and legal due diligence is usually at the end of the process. This phase is last more for reasons of larger number of people involved and cost than for confidentiality reasons

Difference Between Due Diligence and Audit

It needs to be underlined that due diligence is different from audit. Audit is an independent examination and evaluation of the financial statements of an organization with a view to express an opinion thereon. Whereas, due diligence refers to an examination of a potential investment to confirm all material facts of the prospective business opportunity. It involves review of financial and non-financial records as deemed relevant and material. Simply put, due diligence aims to take the care that a reasonable person should take before entering into an agreement or a transaction with another party.

Chapter-VII.2

Approach to Due Diligence

Is this the time to look for things that are wrong with the business? Is this the time to strictly verify numbers? Is this the time to disprove what the investor has been told by the target company? While each of these approaches is somewhat valid none are absolute. While the investor would want to employ a part of each of these strategies, an effective due diligence is when one can really "check things out". This exercise is to be used to determine whether the future looks bright for the business and the industry. To do so, the investor must investigate far more than the financial aspect. Sure, the various financial statements will give the investor a picture of the past and perhaps a glimpse of the future but the past is over and done with. The investor must, therefore, thoroughly review the company's sales, marketing, employees, contracts, customers, competition, systems, suppliers, and legal and corporate issues. The investor wants to complete the due diligence exercise knowing exactly what one is getting into, what needs to be fixed, what the costs are to fix and if one is the right person to be at the helm to put the plans in place to make a great future for the business.

For doing all such exercise the levied down approach to Due Diligence should be followed :

1. Due Diligence Period

Target companies normally try to negotiate the shortest due diligence period possible. However, it is impossible to understand a business in a short time. Even for the smallest of companies, an investor would ordinarily need no less than 20 working days. Since a proper investigation reaches farther than just financials the investor must negotiate for adequate time to accumulate the information. For this purpose, the target company should be clearly communicated all that would be investigated. It should also be made clear to the target company that if it truly wants the deal

to move forward it must allow the potential investor adequate time to do the proper investigations.

2. Preparation

Preparation for due diligence begins the moment it is believed that the business may be worth pursuing. After the investor meets the target company's authorities the first time and believes that one may be interested one should begin to organise one's plan. The first step in this direction is preparing lists and noting areas and specific details related to the business that need further review. Once the investor gets closer to a decision to go for the deal detailed, "to do" lists need to be maintained, broken down for each aspect of the business (i.e., Financials, Employees, Sales, Contracts, etc.). The target company should be kept informed of when the investor anticipates beginning the due diligence. Lists of the materials needed from the target company should be first assembled and never the due diligence exercise should begin until the investor has received all of the supporting documents that one needs from the target company.

3. Getting the Target Company and its Staff to Cooperate

The target company must let its people know that they are to provide one with full access to all files and complete cooperation throughout the investor's investigation.

4. What if Surprises are Found

This should probably be titled: "What to do "WHEN" surprises are found" because this is likely to happen. On the contrary, if surprises are not found, it may imply that the examination has not been thorough enough. The Due Diligence team needs to deal with each on its own and make sure that each is thoroughly investigated so that the facts are foolproof. However, the exercise should not be bogged down with minor issues and these have to be taken as "part of the due diligence package". Unless something is found that cannot be resolved or is so detrimental that even if the target company significantly lowers the acquisition price, the

potential buyer would still walk away from the deal, it is best to take all of these obstacles in stride. Do not publicise them; investigate them. A few issues do not mean that the business is bad. The items or issues must be appropriately weighed with reference to the impact against the future viability of the business. It should be remembered that the goal is to learn what the potential buyer would be getting into and what the future can be with the investor in charge. The option always exists for the investor to renegotiate once the investigation is completed. The investor will be in a much stronger position if one can go to the entrepreneur with very specific concerns, which require reevaluation and renegotiation. With this in mind, the findings should not be discussed with anyone except the accountant or other advisors.

5. Applications

Most business managers routinely develop critical relationships with new suppliers and customers without much forethought. However, making assumptions about the integrity and ethical standards of the customers and suppliers can leave the business vulnerable. Businesses sometimes find themselves in difficult situations that could have been avoided had they conducted thorough background checks. For example, a “friend” might have been hired to run a new startup, not knowing that he had defrauded a former employer. The mistake of giving him sole signing authority on the startup's accounts may result in victimisation about six months later. Another example could be of an individual from another country claiming that he can broker a substantial financing for the potential buyer, who then engages his services. It is, however, subsequently learnt that this engagement is far beyond the scope of his experience and capability, and that there are some unsavory aspects to the people he represents.

6. Integrity Due Diligence

It, is a process of gathering and analysing information to assess whether or not one wants to do business with a person or company. This intelligence will allow one to make informed decisions and can reduce or eliminate any number of possible risks.

There is a host of legal and ethical information available to help one protect oneself and the business. Most people think that checking references or “asking around” is enough. However, when someone provides with a reference, he usually nominates someone he has hand picked. To get a truly objective feedback a different and much deeper approach is needed to be taken. A comprehensive review could include areas such as:

- *Civil Litigation History* - These records are available on a jurisdiction-by- jurisdiction basis, so knowing where to look is very important.
- *Writs Of Execution* - A writ is issued when a judgment has been issued in a civil trial but has not been paid. A writ may be the only evidence of an important case.
- *Criminal Records* - An important check, but it should not stop there. Much of the fraudulent or unethical behaviour in business are civil matters that do not result in criminal prosecution or charges.
- *Current Charges* - A criminal records check will indicate only prior convictions. It also needs to be known if there are any current charges that have not yet gone to court.
- *Corporate Affiliations* - What are other associations? What is the nature of the involvement? What is the history and reputation of these businesses? Commercially available databases of corporate information can help, as can state and national level records.
- *News Media* - A full range of media should be checked; from small local newspapers to the national dailies, as well as industry periodicals and international sources.
- *Internet* - The Internet has provided a publishing medium to the masses. Someone may have communicated information about the potential business partners that is not in the press but from which one might benefit.
- *Credit Reports* - Available through credit-rating companies such as CRISIL, ICRA, etc. credit reports can provide a lot of

useful information on companies and individuals. Personal credit reports are available only with signed consent, but this is not a requirement for obtaining a credit report on a company.

- *Insolvency Filings* - Have the individuals ever filed for, or been petitioned into insolvency ? What were the circumstances?

When Should Integrity Due Diligence Be Considered

When an investor is looking to enter a new business relationship, it should be considered important to conduct background checks. Examples include:

- Reviewing potential suppliers
- Entering into a licensing agreement
- Reviewing prospective joint venture partners
- Entering new markets
- Reviewing existing customers
- Reviewing potential merger or acquisition targets
- Reviewing individuals who wish to broker opportunities for investing company, including financing, property development, new markets, etc.

The time and money invested in integrity due diligence just might save the investor from a significant business risk.

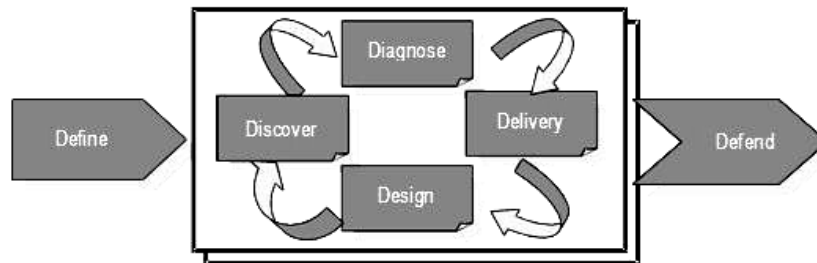
Chapter-VII.3

Work Approach to Due Diligence

The purchase of a business in many instances is the largest and most expensive asset purchase in life time and therefore some caution should be exercised through the due diligence process. Therefore, assessing the businesses fair value passes through:

- Reviewing and reporting on the financials submitted by the target company.
- Assessing the business first hand by a site visit (if applicable).
- Working through the due diligence process with the acquisition company or investor by defining the key areas.
- Helping prepare an offer based on completion of due diligence.

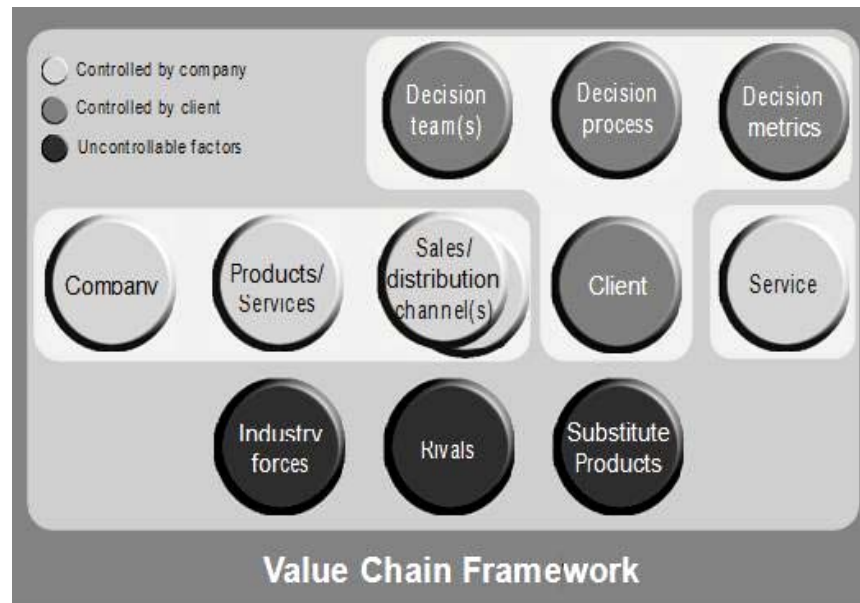
Discovering the correct strategy is always challenging, and even more so during challenging economic circumstances. Each situation is unique. The variables are numerous, including factors such as company age, markets, geography, price levels, competitive dynamics, to name but a few. But when a company and its products are tuned to match market needs and expectations - that is, the decision makers and influencers involved in purchase decision - exceptional changes in performance can occur. However, a comprehensive model that describes this approach to the work is illustrated in the figure below:



Six Dimensional Process Framework

Training Material on Internal Audit

The approach as illustrated in the figure above is further expanded below to clarify the work stages.



It needs to make sure that no hidden time bombs are ticking away in the business proposed to be acquired. The process kicks off when both the buyer and the seller sign a letter of intent, or term sheet, which sets the starting purchase price for a deal. By signing the letter, the seller agrees to open up the target company to a top- to-bottom examination by the buyer and adjust the sale price based on the findings of due diligence. Here is what to keep in mind :

- a) **It is about managing risk.** Double-check financials, tax returns, patents, and customer lists, and make sure the company does not face a lawsuit or criminal investigation. Extra caution needs to be exercised if the company has never undergone an audit from an outside accounting firm. The company's customers can also be quite informative. The seller can be requested for a list of the most favoured clients and these customers can be called up.
- b) **Prioritise the people.** Background checks on the company's key officers should be undertaken.

- c) **Carry out the checks** as listed in Annexure 'A' of Chapter 3 with reference to documents and third part verification, as appropriate.
- d) **Prepare to fix the price.** The investor can and should use any flaws that the due diligence uncovers to negotiate down the sale price. Due diligence is "a chance to get a better deal."

How to Conduct Due Diligence

- a. Start with an open mind. Do not assume that anything wrong will be found and look for it. What needs to be done is to identify trouble spots and ask for explanations.
- b. Get the best team of people. If you do not have a group of people inside your firm that can do the task (e.g. lack of staff, lack of people who know the new business because you are acquiring a business in an unrelated areas, etc.), there are due diligence experts that you can hire. When hiring such professionals look for their experience record in the industry.
- c. Get help in all areas: finance, tax, accounting, legal, marketing, technology, and any others relevant to the assignment so that you get a 36-degree view of the acquisition candidate.
- d. Talk to customers, suppliers, business partners, and employees are great resources.
- e. Take a risk management approach. So while you want to do your research, you also want to make sure that you do not antagonise the team of people of the target company by bogging them down with loads of questions.
- f. Prepare a comprehensive report detailing the compliances and substantive risks/issues.

Examples of Different Approaches

By and large, approach to due diligence exercise follows a common line. However, there are methodologies which different practitioners have developed to adequately cover the salient aspects of due diligence for various types of transactions.

Valuation

Business valuation is another important task in the due diligence exercise. There are many reasons to know the value of the business – if it is considered to buy a business, a merger or outright sale. Whatever the reason for needing to know this information, trying to come up with a valid figure can be a major effort and challenge.

A realistic business valuation requires more than merely looking at last year's financial statement. A valuation requires a thorough analysis of several years of the business operation and an opinion about the future outlook of the industry, the economy and how the subject company will compete.

There are many hard-to-measure intangibles that are a factor in the value of a business. It is not simply a process of adding up the numbers from a variety of reports. Business valuation has been called an art, rather than a science. Estimates of a business' value by various experts can vary as much as 30 percent.

Not only is there no consistency in methods used, but also there is also no consistency in naming the methods. Each method has a variety of names. The important factor in any valuation is that the method used is relevant to your type of business, providing a valid and supportable value.

This wide variety of methods available can be a confusing array to choose from. That is why a professional is often helpful. There are plenty of pros and cons for each method - and there seem to always be new valuation methods being touted.

Make certain a clear explanation of the valuation method is provided and justified. The current business owner needs to understand the possible valuation methods to be able to clearly defend the price of their business. For a buyer or investor, the reasoning behind the pricing is critical for evaluating the personal risk involved. Of critical importance to all parties is a sense of honesty in the method used.

While there is no such thing as absolute truth in business valuation, confidence in the eventual number is based on the integrity of the underlying process. To assure that integrity, many valuation professionals use more than one method, computing a weighted average to arrive at their final number. Following are some common valuation methods.

Adjusted Book Value

It is one of the least controversial valuation methods. It is based on the assets and liabilities of the business.

Asset Valuation

This method is often used for retail and manufacturing businesses because they have a lot of physical assets in inventory. Usually it is based on inventory and improvements that have been made to the physical space used by the business. Discretionary cash from the adjusted income statement can also be included in the valuation.

Capitalisation of Income Valuation

This approach is frequently used by service organisations because it places the greatest value on intangibles while giving no credit for physical assets. Capitalisation is defined as the Return on Investment that is expected. In nutshell, one ranks a lists of variables with a score of 0-5 based on how strong the business is in each of those variables. The scores are averaged for a

capitalisation rate, which is used as multiplication factor of the discretionary income to arrive at the business' value.

Capitalised Earning Approach

This method is based on the rate of return in earnings that the investor expects. For no risk investments, an investor would expect eight percent. Small businesses usually are expected to have a rate of return of 25 percent. Consequently, if the business has expected earnings of say, Rs.50, 000, its value might be estimated at Rs.200, 000 ($200,000 * 0.25 = 50,000$).

Cash Flow Method

This approach is based on how much of a loan one could get based on the cash flow of the business. The cash flow is adjusted for amortization, depreciation, and equipment replacement, then the loan amount calculated with traditional loan business calculations. The amount of the loan is the value of the business.

Cost to Create Approach

This approach is used when the buyer wants to buy an already functioning business to save startup time and costs. The buyer estimates what it would have cost to do the startup less what is missing in this business plus a premium for the saved time.

Debt Assumption Method

This method usually gives the highest price. It is based on how much debt a business could have and still operate; using cash flow to pay the debt.

Discounted Cash Flow

This method is based on the assumption that a rupee received today is worth more than one received in the future. It discounts the business's projected earnings to adjust for real growth, inflation and risk.

Excess Earning Method

This separated from other earnings, which are interpreted as the "excess" earnings you generate. Usually return on assets is estimated from an industry average.

Multiple of Earnings

One of the most common methods used for valuing a business, in this method a multiple of the cash flow of the business is used to calculate its value.

Multiplier or Market Valuation

This method uses an industry average sales figure from recent business sales in comparable businesses as a multiplier. For instance, the industry multiplier for an ad agency might be 75, which is multiplied by annual gross sales to arrive at the value of the business.

Owner Benefit Valuation

Under this method value of business is computed by multiplying 2.2727 times the owner benefit.

Rule of Thumb Methods

This is quick and dirty methods based on industry averages that help give a starting point for the valuation. While not popular with financial analysts, this is an easy way to get a ballpark on what your business might be worth. Many industry organizations provide rule of thumb methods for businesses in their industry.

Tangible Assets (Balance Sheet) Method

This method is often used for businesses that are losing money. The value of the business is based essentially on what the current assets of the business are worth.

Value of Specific Intangible Assets

This method is useful when there are specific intangible assets that come with a business that are highly valuable to the buyer. For example, a customer base would be valuable to an insurance or advertising agency. The value of the business is based on a method similar to the Capitalised Earning Approach, but return on assets is on how much it would have cost the buyer to generate this intangible asset themselves.

Sales Agreement

The sales agreement is the key document in buying the business assets or the stock of a corporation. It is important to make sure the agreement is accurate and contains all of the terms of the purchase. It would be a good idea to have a lawyer review this document. It is in this agreement that everything should be defined that the buyer intends to purchase of the business, assets, customer lists, intellectual property and goodwill.

The following is a checklist of items that should be addressed in the agreement:

- Names of Seller, Buyer and Business
- Background information
- Assets being sold
- Purchase price and Allocation of Assets
- Covenant Not to Compete
- Any adjustments to be made
- The Terms of the Agreement and payment terms
- List of inventory included in the sale
- Any representation and warranties of the seller
- Any representation and warranties of the buyer

- Determination as to the access to any business information
- Determination as to the running of the business prior to closing
- Contingencies
- Possibilities of having the seller continue as a consultant
- Fee - including brokers fees
- Date of closing.

Due Diligence Team

A due diligence team needs multi-discipline expertise. Finance and accounts and legal specialists are the core to be adequately supported by market analyst, environmental expert, human resource specialist and the requisite technology specialist. Hence, it is an association or consortium approach that fits the bill for this exercise. Accordingly, the lead manager for the due diligence exercise has to arrange and organise this team. However, it may be mentioned that the description of the team given should not be taken as sacrosanct as this depends on the type and nature of due diligence. For example, in case of franchisee, finance and legal experts together with a market analyst may be sufficient

Challenges and Risks Covered in Due Diligence Process

The Value of Due Diligence

Prior to engaging in any business relationship, knowledge of the respective company and individuals must be based on facts, not perception. Due diligence findings have to provide conclusive, documented legal information about the target company's litigation history, credit history, business formation and a host of other pertinent information. In this litigious society it is common to identify pending civil litigation not previously revealed, including discrimination, monopolistic practices, and intellectual property lawsuits.

Acquisition due diligence assesses the risks and opportunities of a proposed transaction. It helps to reduce the risk of post-transaction unpleasant surprises. It is vital that the results of any due diligence process are relevant to the transaction including:

- Valuation of the target and therefore the purchase price
- Sale and purchase agreement (e.g. accounting definitions, accounting and tax warranties and indemnities, etc)
- Integration plan (e.g. deal synergies)

There are a range of circumstances in which companies can benefit from externally provided acquisition due diligence, viz.,

- Where any organisation is considering an acquisition, merger or joint venture.
- Where the organisation or deal manager has limited experience in undertaking due diligence.

Challenges and Risks Covered in Due Diligence Process

- Where existing advisers face a conflict of interest, or are not well placed to undertake the necessary due diligence.
- Where the required due diligence demands technical capabilities and commercial experience beyond the organisation's internal resources.

Doing business in emerging markets requires an acute understanding of the unique risks present and an ability to mitigate those risks. Without such an understanding or ability, any business, is exposed to a variety of threats to their operations, assets and profit line.

Having an effective risk management or security programme in place allows a business to protect its bottom line and maintain competitive advantage. The business environments in these markets are all very different, each having its own unique characteristics.

Different Markets, Different Challenges

Each country and its market have different features and therefore different challenges. For example:

- Unfamiliar customs, cultures and languages make understanding and controlling risk difficult.
- Complex regulations, a different legal system and priorities create barriers to enforcement.
- Political and economic change, business closures, rising unemployment and grey markets can create hostile environments.
- Obscured conflicts of interest, intricate personal networks, all make forging business relationships difficult

Different Challenges, Different Risks

These challenges give rise to various risks that need to be searched and examined during the due diligence process. The risks, generally, entail:

- Revenue losses from counterfeit goods, trademark infringements and grey market activity

Training Material on Internal Audit

- Theft of proprietary information and industrial espionage
- Collusion, corruption and fraud
- Loss or damage to physical assets
- Physical threats to employees and their families
- Damage to business reputation from unethical business practices or local contractors and business partners.

Effectively addressing these risks requires any business to possess an acute understanding of the various ethnic, cultural, socio-political and economic factors affecting the business environment.

Culture Aspect

During the due diligence process, especially in case of merger and acquisition, it is equally important to pay attention to what is called human due diligence. Under “human due diligence,” understanding the culture of the organisation, the roles that individuals play, and the capabilities and attitudes of the people are grouped. During the due diligence process, focus requires to be given on identifying key employees to be retained. The new organisation will need the right talent and an integrated, consistent leadership voice to make the merger successful. But when it comes to how to factor in the two cultures into a new organisation, leaders need to identify something more substantive than “decision making styles” to better understand the role of culture in making or breaking the merger. Therefore, a critical element of the due diligence process is an assessment of how well each company is doing in executing key management practices that have been proven to be linked to bottom line results. One company may be stronger in some practices than the other. When working with companies who are looking to merge or acquire the other, it is important to know how the two companies measure up individually in executing these management practices. This assessment tells where the gaps might be that the leaders will need to address before, during, and after the merger. Otherwise it may be merely looking at what is called “culture” and find out only

later that it was more window dressing than substantive business concerns.

This exercise can give both companies a clear picture of how well each of them is doing in four critical areas that reflect both an external and internal focus:

- Adaptability
- Mission
- Consistency
- Involvement

It is a matter of concern in a merger that indicates that neither organisation has a particularly strong ability to adapt to market changes and customer needs (Adaptability) than how similar are the dress codes or benefits packages. Not to say that the merger should be abandoned but instead such an assessment will present the post-merger challenges and risks more clearly and concretely to the decision makers. This makes for a more robust due diligence, focused on the key management practices that will ultimately determine the success of the merger and, more importantly, bottom line business results. Otherwise, the two companies run the risk of falling into the trap of assuming the acquiring company or larger company's culture will be the culture of the new company. This could end up perpetuating, or even exacerbating, the deficient management practices in the new company. Better to find out where each company stands during the due diligence process by asking up front the people who see the company's culture from the inside looking out. No matter how challenging a merger or acquisition can be to the executives in charge, it is that much more complicated in the trenches. All the more reason to concentrate on assessing and understanding the culture from grass roots perspective. Otherwise, leaders retained will squander their talent by assuming culture means one thing when it really means another.

Employee Screening

Security risks to companies are both internal and external. Loss prevention begins internally, with the employee or business

partner, only following that, does it deal with the non-employee and external factors. Hiring employees is one of the most critical business decisions a company makes. Recruiting new staff members on the basis of personal recommendations and appearance is not enough. Experience has taught many businesses that if they had objectively and comprehensively screened candidates prior to employment, many malpractices such as conflict of interest, industrial espionage, theft of proprietary information, contravention of business compliance issues, business fraud might have been avoided.

Employment screening is an essential process to safeguard any business from hiring persons who are either unqualified or of questionable integrity. Screening applicants through pre- and post-hire enquiries is loss prevention in its purest sense. This should not be restricted to employees, as the future problems that choosing an unsuitable business partner or vendor may create, should not be underestimated. To address this issue is due diligence and companies are encouraged to approach suitable professionals who specialise in this and related services, with wide network. This places them in an excellent position to screen emerging market-based applicants who may have studied or resided overseas or worked at companies that are incorporated or headquartered outside of India.

The extent of screening is determined by the seniority or sensitivity of the position to be filled; this also applies to joint venture partners or vendors when checking companies. Screening both existing and new employees at all levels is important. Even the lowest level of employee might have access to proprietary information and processes that are critical to the efficient running of the company. Companies should also consider screening personnel being either relocated to or promoted into areas where they will have additional responsibilities.

The overall objective of employee screening is to “protect” a company against hiring personnel who exaggerate or make false claims about their qualifications, work experience and personal background or, identify weaknesses or withheld information that is relevant to employment such as previous criminal convictions or misconduct.

There should, however, be a balance between the risks involved *vis-a-vis* cost of employee screening. Further, though complexity and budget will vary from company to company, initial outlay can assist in reducing potential for large losses. It is a recognised fact that the soul of any organisation is its people and the company's performance improves by providing care and attention to personnel selection. It is recommended that with any programme embarked upon, screening or background checks must be adapted to job level or size of company to be checked. Selection of an individual or company must be on an objective basis, not a subjective criteria and uniformity of processing is vital if the programme is to succeed, otherwise the programme will be piecemeal and vulnerabilities exist.

For the purpose of due diligence, it is strongly encouraged to contact industry leaders in security who can also be consulted on risk management, commercial enquiries, information security, personal protective services, and many other specialist fields offering premier security consultancy services for a systematic approach to asset protection.

Environment Risk Coverage

Environmental, health and safety (EHS) due diligence is the best way to avoid unforeseen environmental liabilities with new acquisitions.

When carrying out real estate acquisitions, divestitures or stock transactions getting clarity on the environmental, occupational, public health and safety regulations that could influence the investment can be an ordeal. That is why it is imperative to conduct a thorough EHS due diligence assessment before buying a facility or property. EHS due diligence assessment includes the necessary on-site and desk studies for identifying potential environmental liabilities associated with the acquisition, leasing and/or divestiture of real properties. Typically, EHS due diligence is used to determine whether:

- ✓ The facility has or will be able to obtain the right permits to do what it is doing or planning to do.

Training Material on Internal Audit

- ✓ The permits will remain valid.
- ✓ There are any constraints on permit renewal.
- ✓ The facility has implemented the proper systems to ensure compliance.
- ✓ The equipment used on site is safe.
- ✓ The facility has a proper safety track record, etc.

EHS due diligence assessment analyses and outlines the legal ramifications to help ensure the acquisition company or the investor will not be exposed to liability.

Site Contamination, Liabilities and Hidden Costs

Investing in a new business overseas is always a challenge. Focusing on limiting the risk of acquiring contaminated site liabilities may sometimes overshadow the main purpose of the investment - running a viable and sustainable business that meets high environmental and occupational health and safety standards. Therefore, this part of due diligence combines EHS risk assessment and regulatory compliance verification.

Following are just a few examples of issues that companies frequently overlook during a transaction:

- ✓ The absence of an air emission permit.
- ✓ The upcoming expiration of a fire safety certificate.
- ✓ The obsolescence or non-compliance of electrical installations or working equipment.
- ✓ The lack of emergency exits or restrictions on the import or use of an essential raw material.

Further, inspections and analysis, include:

- Subsurface sampling and analysis to confirm the presence or absence of contamination or other problems from soil, surface water and groundwater.

Challenges and Risks Covered in Due Diligence Process

- Building integrity.
- Machinery conformity.

In many countries, these issues can result in significant delays in the start-up of operations. They may also require extensive additional investments to limit the risk of prosecution and other employer liabilities.

Information Technology Security

Majority of the organisations today utilise computer systems for delivery and support of their business. Rapid advances in technology have resulted in deployment of new information technology (IT) systems. Adequate controls are not typically enforced in these systems resulting in higher risks and vulnerabilities. Concern over security, availability and integrity of IT systems is receiving increased attention.

Reviewing key IT components to help ensure the integrity and accuracy of information contained therein is of paramount importance to all areas of business and industry. A comprehensive technical review of the computing environment includes:

- ✓ Operating systems,
- ✓ Network and Connectivity,
- ✓ Vulnerability reviews of business applications,
- ✓ Databases,
- ✓ Change Management,
- ✓ Governance,
- ✓ Risk management,
- ✓ Helpdesk services,
- ✓ Disaster Recovery Plan and Business Continuity Planning.

Training Material on Internal Audit

The assessment methodology should cover the following aspects:

- Aligning business and local statutory requirements/ mandates.
- Performing risk assessment and identify potential risk areas.
- Prioritising and categorise these issues.
- Possible Action plan to remediate potential risk areas.

Conclusion

In sum, in addition to the traditional financial, legal and technical matters, the challenges cited above emerging with change in business environment and globalisation are significant factors that a comprehensive due diligence is required address.

ANNEXURE - A

Sample Due Diligence Checklist

The following due diligence checklist is only a sample, and may differ from the actual list used during the deal process. Some of the information may not be relevant to every situation, and will not be required by the buyer.

A. Organisation of the Company

- 1) Describe the corporate or other structure of the legal entities that comprise the Company. Include any helpful diagrams or charts. Provide a list of the officers and directors of the Company and a brief description of their duties.
- 2) Long-form certificate of good standing and certificate of incorporation. Listing all documents on file with respect to the Company, and a copy of all documents listed therein.
- 3) Current by-laws of the Company (i.e. Articles of Association)
- 4) List of all jurisdictions in which the Company is qualified to do business and list of all other jurisdictions in which the Company owns or leases real property or maintains an office and a description of business in each such jurisdiction. Copies of the certificate of authority, good standing certificates and tax status certificates from all jurisdictions in which the Company is qualified to do business.
- 5) All minutes for meetings of the Company's board of directors, board committees and shareholders for the last five years, and all written actions or consents in lieu of meetings thereof.

- 6) List of all subsidiaries and other entities (including partnerships) in which the Company has an equity interest; organisational chart showing ownership of such entities; and any agreements relating to the Company's interest in any such entity.

B. Ownership and Control of the Company

1. Capitalisation of the Company, including all outstanding capital stock, convertible securities and similar instruments.
2. List of shareholders of the Company, setting forth class and number of shares held.
3. Copies of any voting agreements, shareholder agreements, proxies, transfer restriction agreements, rights of first offer or refusal, pre-emptive rights, registration agreements or other agreements regarding the ownership or control of the Company.

C. Assets and Operations

1. Annual financial statements with notes thereto for the past three fiscal years of the Company, and the latest interim financial statements since the end of the last fiscal year and product sales and cost of sales (including royalties) analysis for each product which is part of assets to be sold.
2. All current budgets and projections including projections for product sales and cost of sales.
3. Any auditor's (internal and external) letters and reports to management for the past five years (and management's responses thereto).
4. A detailed breakdown of the basis for the allowance for doubtful accounts.
5. Inventory valuation, including turnover rates and statistics, gross profit percentages and obsolescence

Challenges and Risks Covered in Due Diligence Process

analysis including inventory of each product, which is part of assets to be sold.

6. Letters to auditors from outside counsel.
7. Description of any real estate owned by the Company and copies of related deeds, surveys, title insurance policies (and all documents referred to therein), title opinions, certificates of occupancy, easements, deeds of trust and mortgages.
8. Schedule of significant fixed assets, owned or used by the Company, including the identification of the person holding title to such assets and any material liens or restrictions on such assets.
9. Without duplication of separate intellectual property due diligence checklist from Section D below, schedule of all intangible assets (including customer lists and goodwill) and proprietary or intellectual properties owned or used in the Company, including a statement as to the entity holding title or right to such assets and any material liens or restrictions on such assets, include on and off balance sheet items.

D. Intellectual Property

List of all patents, trademarks, service marks and copyrights owned or used by the Company, all applications and copies thereof, search reports related thereto and information about any liens or other restrictions and agreements on or related to any of the foregoing.

E. Reports

1. Copies of any studies, appraisals, reports, analysis or memoranda within the last three years relating to the Company (i.e. competition, products, pricing, technological developments, software developments, etc.)

2. Current descriptions of the Company that may have been prepared for any purpose, including any brochures used in soliciting or advertising.
3. Descriptions of any customer quality awards, plant qualification/ certification distinctions, ISO certifications or other awards or certificates viewed by the Company as significant or reflective of superior performance.
4. Copies of any analyst or other market reports concerning the Company known to have been issued within the last three years.
5. Copies of any studies prepared by the Company regarding the Company's insurance currently in effect and self-insurance programme (if any), together with information on the claim and loss experience there under.
6. Any of the following documents filed by the Company or affiliates of the Company and which contain information concerning the Company i.e., annual reports, and quarterly reports.

F. Compliance with Laws

1. Copies of all licences, permits, certificates, authorisations, registrations, concessions, approvals, exemptions from all governmental and other operating authorities any applications therefore, and a description of any pending contemplated or threatened changes in the foregoing.
2. A description of any pending or threatened proceedings or investigations before any court or any regulatory authority.
3. Describe any circumstance where the Company has been or may be accused of violating any law or failing to possess any material licence, permit or other authorisation. List all citations and notices from governmental or regulatory authorities.

Challenges and Risks Covered in Due Diligence Process

4. Schedule of the latest dates of inspection of the Company's facilities by each regulatory authority that has inspected such facilities.
5. Description of the potential effect on the Company of any pending or proposed regulatory changes of which the Company is aware.
6. Copies of any information requests from, correspondence with, reports of or to, filings with or other material information with respect to any regulatory bodies, which regulate a material portion of the Company's business. Limit response to the last five years unless an older document has a continuing impact on the Company.
7. Copies of all other studies, surveys, memoranda or other data on regulatory compliance including, spill control, environmental clean-up or environmental preventive or remedial matters, employee safety compliance, import and export licences, common carrier licences, problems, potential violations, expenditures, etc.
8. State whether any consent is necessary from any governmental authority to embark upon or consummate the proposed transaction.
9. Schedule of any significant import or export restrictions that relate to the Company's operations.
10. List of any export, import or customs permits or authorisations, certificates, registrations, concessions, exemptions, etc., that are required in order for the Company to conduct its business and copies of all approvals, etc. granted to the Company that are currently in effect or pending renewal.
11. Any correspondence with or complaints from third parties relating to the marketing, sales or promotion practices of the Company.

G. Environmental Matters

1. A list of facilities or other properties currently or formerly owned, leased, or operated by the Company and its predecessors, if any.
2. Reports of environmental audits or site assessments in the possession of the Company.
3. Copies of any inspection reports prepared by any governmental agency or insurance carrier in connection with environmental or workplace safety and health regulations relating to any such facilities or properties.
4. Copies of all environmental and workplace safety and health notices of violations, complaints, consent decrees, and other documents indicating non-compliance with environmental or workplace safety and health laws or regulations, received by the Company from local, state, or central governmental authorities. If available, include documentation indicating how such situations were resolved.
5. Copies of any private party complaints, claims, lawsuits or other documents relating to potential environmental liability of the Company to private parties.
6. Listing of underground storage tanks currently or previously present at the properties and facilities listed in response to item 1 above, copies of permits, licences or registrations relating to such tanks, and documentation of underground storage tank removals and any associated remediation work.
7. Descriptions of any release of hazardous substances or petroleum known by the Company to have occurred at the properties and facilities listed in response to Item 1, if such release has not otherwise been described in the documents provided in response to Items 1-6 above.

Challenges and Risks Covered in Due Diligence Process

8. Copies of any information requests, or other notices received by the Company relating to liability for hazardous substance releases at off-site facilities.
9. Copies of any notices or requests described in Item 8 above, relating to potential liability for hazardous substance releases at any properties or facilities described in response to Item 1.
10. Copies of material correspondence or other documents (including any relating to the Company's share of liability) with respect to any matters identified in response to Items 8 and 9.
11. Copies of any written analyses conducted by the Company or an outside consultant relating to future environmental activities (i.e., upgrades to control equipment, improvements in waste disposal practices, materials substitution) for which expenditure significant amount is either certain or reasonably anticipated within the next five years and an estimate of the costs associated with such activities.
12. Description of the workplace safety and health programmes currently in place for the Company's business, with particular emphasis on chemical handling practices.

H. Litigation

1. List of all litigation, arbitration and governmental proceedings relating to the Company to which the Company or any of its directors, officers or employees is or has been a party, or which is threatened against any of them, indicating the name of the court, agency or other body before whom pending, date instituted, amount involved, insurance coverage and current status. Also describe any similar matters which were material to the Company and which were adjudicated or settled in the last ten years.

2. Information as to any past or present governmental investigation of or proceeding involving the Company or the Company's directors, officers or employees.
3. Copies of any consent decrees, orders (including applicable injunctions) or similar documents to which the Company is a party, and a brief description of the circumstances surrounding such document.
4. Copies of all letters of counsel to independent public accountants concerning pending or threatened litigation.
5. Any reports or correspondence related to the infringement by the Company or a third party of intellectual property rights.

I. Significant Contracts and Commitments

1. Contracts relating to any completed (during the past 10 years) or proposed reorganisation, acquisition, merger, or purchase or sale of substantial assets (including all agreements relating to the sale, proposed acquisition or disposition of any and all divisions, subsidiaries or businesses) of or with respect to the Company.
2. All joint venture and partnership agreements to which the Company is a party.
3. All material agreements encumbering real or personal property owned by the Company including mortgages, pledges, security agreements or financing statements.
4. Copies of all real property leases relating to the Company (whether the Company is lessor or lessee), and all leasehold title insurance policies (if any).
5. Copies of all leases of personal property and fixtures relating to the Company (whether the Company is lessor or lessee), including, without limitation, all equipment rental agreements.

Challenges and Risks Covered in Due Diligence Process

6. Guarantees or similar commitments by or on behalf of the Company, other than endorsements for collection in the ordinary course and consistent with past practice.
7. Indemnification contracts or arrangements insuring or indemnifying any director, officer, employee or agent against any liability incurred in such capacity.
8. Loan agreements, lines of credit, lease financing arrangements, installment purchases, etc. relating to the Company or its assets and copies of any security interests or other lines securing such obligations.
9. No-default certificates and similar documents delivered to lenders for the last five (or shorter period, if applicable) years evidencing compliance with financing agreements.
10. Documentation used internally for the last five years (or shorter time period, if applicable) to monitor compliance with financial covenants contained in financing agreements.
11. Any correspondence or documentation for the last five years (or shorter period, if applicable) relating to any defaults or potential defaults under financing agreements.
12. Contracts involving cooperation with other companies or restricting competition.
13. Contracts relating to other material business relationships, including:
 - a) any current service, operation or maintenance contracts;
 - b) any current contracts with customers;
 - c) any current contracts for the purchase of fixed assets; and
 - d) any franchise, distributor or agency contracts

Training Material on Internal Audit

14. Without duplicating the intellectual property due diligence check list as outlined in Section D above, contracts involving licensing, know-how or technical assistance arrangements including contracts relating to any patent, trademark, service mark and copyright registrations or other proprietary rights used by the Company and any other agreement under which royalties are to be paid or received.
15. Description of any circumstances under which the Company may be required to repurchase or repossess assets or properties previously sold.
16. Data processing agreements relating to the Company.
17. Copies of any contract by which any broker or finder is entitled to a fee for facilitating the proposed transaction or any other transactions involving the Company or its properties or assets.
18. Management, service or support agreements relating to the Company, or any power of attorney with respect to any material assets or aspects of the Company.
19. List of significant vendor and service providers (if any) who, for whatever reason, expressly decline to do business with the Company.
20. Samples of all forms, including purchase orders, invoices, supply agreements, etc.
21. Any agreements or arrangements relating to any other transactions between the Company and any director, officer, shareholder or affiliate of the Company (collectively, "Related Persons"), including but not limited to:
 - a) Contracts or understandings between the Company and any Related Person regarding the sharing of assets, liabilities, services, employee benefits, insurance, data processing, third-

Challenges and Risks Covered in Due Diligence Process

party consulting, professional services or intellectual property.

- b) Contracts or understandings between Related Persons and third parties who supply inventory or services through Related Persons to the Company.
 - c) Contracts or understandings between the Company and any Related Person that contemplate favourable pricing or terms to such parties.
 - d) Contracts or understandings between the Company and any Related Person regarding the use of hardware or software.
 - e) Contracts or understandings regarding the maintenance of equipment of any Related Person that is either sold, rented, leased or used by the Company.
 - f) Description of the percentage of business done by the Company with Related Persons.
 - g) Covenants not to compete and confidentiality agreements between the Company and a Related Person.
 - h) List of all accounts receivable, loans and other obligations owing to or by the Company from or to a Related Person, together with any agreements relating thereto.
22. Copies of all insurance and indemnity policies and coverages carried by the Company including policies or coverages for products, properties, business risk, casualty and workers compensation. A summary of all material claims for the last five years as well as aggregate claims experience data and studies.
23. List of any other agreements or group of related agreements with the same party or group of affiliated

Training Material on Internal Audit

parties continuing over a period of more than six months from the date or dates thereof.

24. Copies of all supply agreements relating to the Company and a description of any supply arrangements.
25. Copies of all contracts relating to marketing and advertising.
26. Copies of all construction agreements and performance guarantees.
27. Copies of all secrecy, confidentiality and non-disclosure agreements.
28. Copies of all agreements related to the development or acquisition of technology.
29. Copies of all agreements outside the ordinary course of business.
30. Copies of all warranties offered by the Company with respect to its products or services.
31. List of all major contracts or understandings not otherwise previously disclosed under this section, indicating the material terms and parties.
32. For any contract listed in this Section state whether any party is in default or claimed to be in default.
33. For any contract listed in this Section state whether the contract requires the consent of any person to assign such contract or collaterally assign such contract to any lender.

NOTE: Remember to include all amendments, schedules, exhibits and side letters. Also include brief description of any oral contract listed in this Section.

J. Employees, Benefits and Contracts

1. Copies of the Company's employee benefit plans as most recently amended, including all pension, profit sharing, thrift, stock bonus, ESOPs, health and welfare plans (including retiree health), bonus, stock option plans, direct or deferred compensation plans and severance plans, together with the following documents:
 - a) all applicable trust agreements for the foregoing plans;
 - b) copies of all determination letters of tax authorities for the foregoing qualified plans;
 - c) latest copies of all summary plan descriptions, including modifications, for the foregoing plans;
 - d) latest actuarial evaluations with respect to the foregoing defined benefit plans; and
 - e) schedule of fund assets and unfounded liabilities under applicable plans
2. Copies of all employment contracts, consulting agreements, severance agreements, independent contractor agreements, non-disclosure agreements and non-compete agreements relating to any employees of the Company.
3. Copies of any collective bargaining agreements and related plans and trusts relating to the Company (if any). Description of labour disputes relating to the Company within the last three years. List of current organisational efforts and projected schedule of future collective bargaining negotiations (if any).
4. Copies of all employee handbooks and policy manuals.
5. The results of any formal employee surveys.

K. Tax Matters

1. Copies of returns for the three prior closed tax years

and all open tax years for the Company together with a work paper therefore wherein each item is detailed and documented that reconciles net income as specified in the applicable financial statement with taxable income for the related period.

2. Audit and revenue agents reports for the Company; audit adjustments proposed by the Tax Authorities for any year of the Company or protests filed by the Company.
3. Settlement documents and correspondence for last six years involving the Company.
4. Agreements waiving statute of limitations or extending time involving the Company.
5. Description of accrued withholding taxes for the Company.

L. Miscellaneous

1. Information regarding any material contingent liabilities and material unasserted claims and information regarding any asserted or unasserted violation of any employee safety and environmental laws and any asserted or unasserted pollution clean-up liability.
2. List of the ten largest customers and suppliers for each product or service of the Company.
3. List of major competitors for each business segment or product line.
4. Any plan or arrangement filed or confirmed under the bankruptcy laws.
5. A list of all officers, directors and shareholders of the Company.
6. All annual and interim reports to shareholders and any other communications with them.
7. Description of principal banking and credit relationships (excluding payroll matters), including the names of

Challenges and Risks Covered in Due Diligence Process

each bank or other financial institution, the nature, limit and current status of any outstanding indebtedness, loan or credit commitment and other financing arrangements.

8. Summary and description of all product, property, business risk, employee health, group life and key-man insurance.
9. Copies of any judgment or suit searches or filings related to the Company in different states conducted in the past three years.
10. Copies of all filings with the Securities Exchange Board of India or foreign security regulators or exchanges.
11. All other information material to the financial condition, business, assets, prospects or commercial relations of the Company.

ANNEXURE B

Specimen Check List For Commercial Due Diligence

Please prepare a folder containing the information requested below. This checklist is to be placed at the top of the folder and should indicate against each question either an explanation or the reference number of the document in the folder that supports the explanation or both. In case a question is not applicable please indicate as such. All documents in the folder should be numbered and the folder should be indexed.

1. General

- i. List of companies/firms which are a part of the business group to which the target company belongs.
- ii. Brief note on the history of the company being invested in, including reference to its foundation and expansion.
- iii. Brief note on present business and activities, including list of business locations; please provide details for separate product/service verticals embedded solutions, infrastructure for power and software solutions.
- iv. Any recent reports on the company's activities prepared internally or by outside consultants (such as analyst reports, information memorandum, valuation reports etc.).
- v. Copies of any literature prepared by the company illustrating its products, operations, history etc.
- vi. Any agreements or documents recording arrangements between shareholders of the company.
- vii. A list of all licenses and registrations held by the company specifying number, validity period, purpose,

Challenges and Risks Covered in Due Diligence Process

granting authority and other relevant details. Copies of the same may also be enclosed.

- viii. Minutes of meetings of the board of directors, shareholders and audit/operational committees since incorporation.
- ix. Brief note on the internal control environment in the division.
- x. Details of bankers, lawyers, consultants and other professional advisers.
- xi. Transactions/agreements with affiliates and related parties especially with respect to prices, payment terms, etc.
- xii. All statutory registers and returns filed required to be maintained/filed under the Companies Act.
- xiii. Details of intellectual property rights (including trademarks and brands) held by the company, if any.
- xiv. Note on planning and control systems prevalent in the organisation including controls over non financial systems such as production planning, quality control, inventory management, sales etc.
- xv. Details of statutory records maintained under the Companies Act and other applicable statutes.
- xvi. Transaction documents (agreements) for any prior acquisitions done by the company or investments in the company.

2. Financial Statements information for the year ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.

- i. Audited/un-audited financial statements of the Company along with its reconciliation with

Training Material on Internal Audit

management accounts for the year ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.

- ii. Chart of accounts.Accounting policy at present, in
- iii. particular with respect to income/sales recognition, research and development, exceptional and extraordinary items, acquisition and disposal of assets, differentiating between capital expenditure and repairs and maintenance, valuation of fixed assets, capitalisation of interest, inventory/stock valuation, transfer pricing, preliminary expenses.
- iv. Details of changes in accounting policies over last 5 years.
- v. Closing audit working files prepared by the Company, as appropriate.
- vi. Trail Balance, schedules and groupings supporting the financial statements for the year ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.
- vii. Audit management letters for the period under review.
- viii. Internal audit reports for the period under review.
- ix. Budgets, comparison with actuals and explanation for variances for last two accounting periods i.e. FY0-, FY0- and YTD0-. Specifically revenue forecast versus. actuals, expenditure forecast versus. actuals and manpower budget versus. actual headcount.
- x. Cash flow statements for the year ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.

3. Management Accounts

- i. Copies of monthly management accounts since April 200_ till date.
- ii. Breakdown of above by vertical (separately identifying financials for embedded solutions, infrastructure for power and software solutions).
- iii. Reconciliation of management accounts to statutory accounts for the year ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.
- iv. Trading Results.

4. Revenues

- i. Split of revenue:
 - ◆ Customer wise,
 - ◆ Product wise/ Service Wise,
 - ◆ Substation Controllers,
 - ◆ Distribution Transformer Monitoring System,
 - ◆ Theft Detection Device,
 - ◆ Intelligent Automatic Meter Reading,
 - ◆ General Automatic Meter Reading,
 - ◆ Spot Billing Machine,
 - ◆ Computerised Online Data Logging System,
 - ◆ Energy Audit Services,
 - ◆ Micro RTU,

Training Material on Internal Audit

- ◆ Vertical wise,
 - ◆ Embedded Solutions,
 - ◆ Infrastructure for Power,
 - ◆ Software Solutions,
 - ◆ Geography wise and target industry sector,
 - ◆ Rural electrification,
 - ◆ Transmission,
 - ◆ Oil and gas,
 - ◆ Technology, and
 - ◆ Exports.
- ii. Historic product/service wise contributions earned and gross margin. Also provide details of direct costs. Details of profitability for top 5 customers.
 - iii. Comparison of revenue and contribution reflected in the finance financial statements with the Management Information System ('MIS') and budgets; analysis of reasons for variance.
 - iv. Average realisations by product/service in last three years for the customers.
 - v. Details of the basis for revenue recognition for all the contracts with customers.
 - vi. Details of deferred revenues year ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_ and bookings carried forward to the next year and the next period.
 - vii. Details on marketing and pricing strategies of the Company; average realisation per hour per contract/

Challenges and Risks Covered in Due Diligence Process

agreement for each key customer/product/service of the Company.

- viii. Revenue per headcount, together with details of employee productivity (monthly data) for the historic period.
- ix. Discount structures and credit terms for major customers; historic average realization per headcount/service for that customer.
- x. Details of customer agreements terms, value, rates, penalties, Service Level Agreements, committed headcount and volume and bearing of training costs. Also provide details of revenue by nature of billing cycle, frequency of billing, milestone based or man hours per month basis/transaction.
- xi. Product wise/service wise/customer wise status of contracts under negotiation and details of the progress in the same.
- xii. Details of customer acquisitions in the last two years ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.
- xiii. Details of customer attrition rate; clients acquired from competitors and clients lost to competitors along with the reasons for the same over the past for the year ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.
- xiv. What has been the increase in the size of operation for the existing clients?
- xv. Details of other income.
- xvi. Details of exceptional and extraordinary income items.
- xvii. Pricing movements for the defined historical period together with the nature of movement; pricing

differences between clients and reasons for the same;
pricing band service wise/product wise, if any.

- xviii. Budget/Actual analysis of product/service-wise and customer wise sales and analysis of the reasons for variations.
- xix. Revenue sharing arrangements and transfer pricing amongst the Divisions, if any as per the terms of the respective contracts.
- xx. Comparison of revenue and contribution reflected in the financial statements with the Management Information System (MIS) and budgets.

5. Customers and Marketing

- i. Write up on selling and distribution methods (systems and procedures followed, *etc*), factors affecting prices, margins, periods of peak and low revenue, *etc*.
- ii. Details on marketing and pricing strategies of the Company.
- iii. Details of various components of freight, tax and other costs from factory sales point to the sale point of the customer.
- iv. Discount structures and credit terms for major customers; historic average price realizations.
- v. Average price realisation (monthly) per unit for each product of the Company in the last two years i.e. March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.
- vi. List of all significant marketing agreements and contracts with customers.
- vii. List of major customers for individual products along with details of geographic segments sales (domestic

Challenges and Risks Covered in Due Diligence Process

and export) for March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.

- viii. Pricing policy for sale to related parties.
- ix. List of any claims/disputes with or complaints from customers giving amounts and background.
- x. Details of all returns by customers with reasons for year ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_.
- xi. List of all competitors, company market share (present and anticipated), etc.
- xii. Status of order book as on December 31, 200_.

6. Suppliers

- i. Purchase policies and procedures.
- ii. List of major suppliers in the period ended March 31, 200_, March 31, 200_ and for the nine months ended December 31, 200_ showing nature of purchase, quantity purchased and amount of purchases.
- iii. Pricing policy for purchases from related companies.
- iv. List of all significant contracts with the suppliers.
- v. Details of purchase at forward prices and forward purchase, if any.
- vi. List of any claims/disputes with suppliers giving amounts and background.

7. Purchases and Consumption Costs.

- i. Material expenditure with the respective supply contracts.

- ii. Consumption costs for individual products; details of actual consumption with standard.
- iii. Details of the power and fuel cost with respect to. unit rates and consumption patterns in the last three years.

8. Expenditure

- i. Details of average headcount cost per customer/service.
- ii. Details of average direct cost per customer/service.
- iii. Direct costs for individual services detailing all components of costs.
- iv. Details of cost structure, breaking it into fixed costs and variable costs.
- v. Personnel cost including perquisites and retirement benefits.
- vi. Details of incentive/commission policy for sales and other of the Company and details of the cost during the historical period.
- vii. Payment of royalty/ technical know-how fees, if any, along with the terms of the respective agreements.
- viii. Details of repairs, rent, stores and spares consumed, carriage and freight, finished goods handling expenses, other expenses, etc.
- ix. Details of the inventory write-offs in the last three years.
- x. Details of provision for bad and doubtful debts in the last three years.
- xi. Administrative and other expenses including professional, legal fees, other expenses.

Challenges and Risks Covered in Due Diligence Process

- xii. Details of the selling and marketing costs.
- xiii. Basis for allocation of common costs and support expenses.
- xiv. Details of financial costs including interest, lease rent and hire charges.
- xv. Details of payment of royalty/ technical know-how fees along with terms of respective agreements.
- xvi. Details of provision for bad and doubtful debts in the last three years.
- xvii. Balance sheet (Details required as on March 31, 2005-, March 31, 200_ and for the nine months ended December 31, 200_, unless otherwise specified).

9. Fixed Assets

- i. Summary showing principal categories of assets at last year end and most recent accounting date showing cost, accumulated depreciation, net book value and depreciation charge for the period.
- ii. Details of valuation/revaluation of fixed assets, if any.
- iii. Details of charges or lien created against any fixed assets through guarantees or loan arrangements.
- iv. Details of insurance policies and coverage of fixed assets.
- v. Details of capital work in progress, if any.
- vi. Contracts for pending capital commitments at last year-end and most recent date - contracted for and authorised but not contracted.
- vii. Copies of leasehold agreements (lease and sub-leases) and tenancy rights, title deeds and other agreements giving amounts and terms involved (renewal options for the lease period).

- viii. Fixed assets ledger/register and supporting documents for fixed assets.
- ix. Physical verification reports and its periodicity.
- x. Procedure for authorising and procurement of capital expenditure.
- xi. Accounting policy for capitalisation of financial costs and details of capitalisation of financial costs.
- xii. Terms and accounting practice for leased/hired assets; details of financing arrangements and payments thereof and details of future commitments, if any.
- xiii. Useful life of assets and depreciation computation.
- xiv. Details of sale of fixed assets and policy for determining prices.
- xv. List of obsolete and idle equipment with cost and net book value attached.
- xvi. List of fully depreciated assets.
- xvii. Details of any restriction on the use or sale of any asset.
- xviii. Foreign exchange fluctuation and accounting thereof.
- xix. List of all properties owned or operated that are connected to the business with details of their book values, usage, title/ lease and rent details.

10. Inventories

- i. Details of inventory/stock as on March 31, 200__, March 31, 2006- and December 31, 2006
- ii. Inventory details and classification into raw materials; work in process, finished goods and stores and spares.

Challenges and Risks Covered in Due Diligence Process

- iii. Quantitative reconciliation of opening stock, purchases, sales and wastage, etc. for FY 0-, FY 0- and YTD 0_.
- iv. Inventory valuation workings and its basis. Details of overhead and other costs included in stock values.
- v. Age wise details of inventory as on March 31, 200_ and March 31, 200_.
- vi. Provisioning policy of inventory and details of provision against inventory as on March 31, 200_ and on December 31, 200_.
- vii. Procedure for identification of slow moving and obsolete/unusable inventories.
- viii. Treatment of goods in transit and material at third location and details in respect thereof as on March 31, 200_, March 31, 200_ and December 31, 200_.

11. Receivables

- i. Party-wise break-up of Sundry Debtors with confirmation and reconciliation statements as on March 31, 200_, March 31, 200_ and December 31, 200_.
- ii. Ageing details of Debtors as on March 31, 200_, March 31, 200_ and December 31, 200_.
- iii. Details of Subsequent receipts with supporting documents.
- iv. Details of credit terms as per the respective contracts and other supporting documents with details of changes in the credit terms, if any.
- v. Details of provisions for doubtful debts/written off debts and movement in provisions since incorporation.
- vi. Details of subsequent receipts with supporting documents.

- vii. Details of dispute in payment/claims filed by customer.
- viii. Details of actual collections period versus contractual credit period for receivables outstanding.
- ix. Details of write off of bad debts over the last three years ended on March 31, 0- or later financial period as being followed.
- x. Nature and details of transactions with related Company and accounts ledger of these receivables.

12. Loans and Advances and Other Current Assets

- i. Details of Advances recoverable in cash or in kind or value to be received with supporting documents as on March 31, 200_, March 31, 200_ and December 31, 200_. Reasons for advancement, ageing, existence and adequacy of contracts and reasonableness of terms and conditions of each receivable.
- ii. Details of deposits with Public Bodies and others prepaid expenses with supporting documents and balance confirmations. Review of the terms of the deposits, ageing and subsequent clearances thereof.
- iii. Details of Fixed Deposits held for disposal and interest accrued on investments and deposits.
- iv. Details of provision for doubtful advances, if any.
- v. Details of amounts due from staff and officers and their subsequent clearances.
- vi. Details of other receivables on account including reason for advancement, ageing, existence and adequacy of contracts and reasonableness of terms and conditions of each receivable.
- vii. Nature and details of transactions with related company and accounts ledger of these receivables.

13. Cash and Bank Balances

- i. List of bank balances and bank accounts as on March 31, 200_, March 31, 200_ and December 31, 200_.
- ii. Bank reconciliation statements and confirmations as on March 31, 200_ and December 31, 200_.
- iii. Details of the fixed deposit amount providing the date of deposit, interest rates, *etc.*

14. Miscellaneous Expenditure to the Extent Not Written-off

Details of accumulated amortization and net book value as on, March 31, 200_, March 31, 200_ and December 31, 200_.

15. Creditors and Accrued Expenses

- i. List of trade creditors at March 31, 200_, March 31, 200_ and December 31, 200_.
- ii. Ageing details of trade creditors along with supply contracts (including the terms of payments) and subsequent payments.
- iii. Contracts with the Vendors.
- iv. Creditors balance confirmation certificates and reconciliation statements as at March 31, 200_, March 31, 200_ and December 31, 200_ or any other latest date.
- v. Details of accruals with supporting documents and subsequent clearances.
- vi. Details of off Balance Sheet Liabilities (such as leases).
- vii. Details of advances received with aging details, subsequent clearances, *etc.*
- viii. Basis of accruals of expenses and other liabilities.

- ix. Details of provisions against claims, if any.
- x. Hedging policy, if any and details of purchase commitments as on date of financial statements.
- xi. Detailed listing of overdue payables.
- xii. Details of any penalties/interest levied on overdue payments, if any.
- xiii. Purchase policies and procedures for all operational (ex: content) and administrative purchases (miscellaneous purchases).
- xiv. List of major suppliers in the period showing nature of contract and value of purchases.
- xv. Pricing policy for purchases from related companies.
- xvi. List of any claims/disputes with suppliers, background and current status of the same.
- xvii. Any redundancy or liability clauses against the key suppliers like transportation, food, Server and Switch maintenance vendors etc.

16. Amounts Due to Related Parties

Nature and details of related company dues and account listing of these dues since the incorporation of the Company

17. Secured and Unsecured Loans

- i. Details and terms of working capital loans and other financing from banks and other parties with their respective repayment schedule. Review of the outstanding amounts at March 31, 200_, March 31, 200_ and December 31, 200_, current interest rates, period, loan covenants.
- ii. Provide details of default in repayment of loans and interest in the historic period, if any.
- iii. Bank facility letters for encumbrances on assets.

Challenges and Risks Covered in Due Diligence Process

- iv. Details of outstanding amounts, current interest rates, period, loan covenants.
- v. Details of any corporate/ personal guarantee extended.
- vi. Confirmation from the Bank on the amount outstanding and interest accrued thereon.
- vii. Details of the sales tax deferral scheme, if any.

18. Reserves

- i. Provide details of all the reserves at the historic balance sheet dates for the historical period. Provide the terms for the statutory reserves.
- ii. For all reserves, provide details regarding (i) purpose of reserve, (ii) period reserves were originally established, and (iii) all movements to the reserve (i.e., roll forward payments against, reversals, transfers, and reclassifications) for each period during the historical period.

19. Contingencies

- i. Significant contracts, correspondence with solicitors, tax offices, shareholders register.
- ii. Details of claims against the Company not acknowledged as debt.
- iii. Details of outstanding bank guarantees and bill discounted.
- iv. List of charges, pledges, etc. over assets of group.
- v. Details of capital commitments, non-cancellable operating lease and other commitments and contingencies.
- vi. Details of litigation disputes against the company, promoters and group concerns on the company.

- vii. List and details of any existing and potential lawsuits/claims - cause, amounts involved, latest provisions, etc.
- viii. Disputes/claims with respect to employees, ex-employees, customers, vendors, etc.
- ix. Details of any regulatory claims against the Company.
- x. Confirmation from the lawyers about the list of legal issues and current status of the same.
- xi. List of any claims/disputes with or complaints from customers giving amounts and background.

20. Secretarial Records

- i. Minutes of Board of Directors and Shareholders meetings.
- ii. Shareholders register.
- iii. Register of Directors and Contracts in which Directors are interested.

21. Human Resources

- i. Organization structure and reporting relationships as on March 31, 200_ and on March 31, 200_.
- ii. Number of employees, grade-wise in each of the vertical and by department.
- iii. Details of time management system, together with details of employee productivity over the historic period.
- iv. List of directors, officers, senior staff (considered key to the business) showing position, name, age, length of service, skills, salary benefits, etc.
- v. HR systems prevalent in the organization, including performance appraisal systems.

Challenges and Risks Covered in Due Diligence Process

- vi. Level-wise headcount movement i.e. month-wise number of employees joining and leaving the organisation in the last two years, by department/function. Also provide us with an average replacement time and cost of replacement.
- vii. Employee contracts, service agreements.
- viii. Details of employee union activities and note explaining significant Union activities since incorporation.
- ix. Details of any wages/bonus, etc. agreements signed with the employee unions.
- x. Staff movement i.e. month-wise number of employees joining and leaving the organisation in the last two years.
- xi. Details of key employees who have left the Company in the past two years.
- xii. Is manpower hired from third parties? If so, agreements with these parties.
- xiii. List of all labor disputes pending as on March 31, 2006 and on December 31, 200_.
- xiv. Employee Provident Fund registration certificate, sample monthly remittance challans,
- xv. annual returns and correspondence with the relevant authorities.
- xvi. Details of accrual of various retirement liabilities viz. leave encashment, gratuity, etc. as on March 31, 200_ and on December 31, 200_. Please also specify how the various retirement benefit liabilities are funded.
- xvii. Actuary certificate for the retirements benefits as on December 31, 200_.
- xviii. Number of employees education wise at the agent and management level.

- xix. The details of the training calendar for the year ended March 31, 200_, March 31, 200_ and the nine months ended December 31, 200_.
- xx. Ratio of full time employed/contracted headcount year ended March 31, 200_, March 31, 200_ and the nine months ended December 31, 200_.
- xxi. Training cost/headcount

22. Forecast

Details of the forecast for FY 200_ (reflecting actuals YTD) and FY 200_ along with detailed assumption on growth assumed in product/service/customer sales, prices, product-wise sales and margins, customers, geographical sales, sales and marketing costs, customer returns, raw material mix-quantity and prices, other administrative costs, interest cost, etc.

Others

23. Technology

- i. Note on the Information technology and the overall control environment of the Company.
- ii. Details of software used for staffing and scheduling, planning and any other key softwares used for the year ended March 31, 200_, March 31, 200_ and the nine months ended December 31, 200_ and what is the efficiency of the scheduling for the top 5 customers.
- iii. Are there any knowledge management software being used for the operations and their details.
- iv. How many licenses are available for different software being used?
- v. Do you have any documented and implemented Disaster Recovery and Business Continuity plan.

Challenges and Risks Covered in Due Diligence Process

- vi. When was last BCP\DRP test performed and details of the same.

24. Infrastructure

- i. What has been the build up of capacity over the last for the last two years i.e. for the year ended March 31, 200_, March 31, 200_ and the nine months ended December 31, 200_.
- ii. What % is the un-utilised capacity?

25. Taxes

Direct Taxes

Summary Information

Year-wise summary chart for income tax and wealth tax for past five years, detailing the following:

- a. Current assessment/ litigation status.
- b. Key disallowances/issues raised by the authorities.
- c. Amount of demands raised by the authorities and paid by the Company.
- d. Level of settlement of dispute (i.e. CIT (A)/ ITAT/ HC/ SC).
- e. Taxable profit/ carried forward loss for the year and set off in future years.
- f. Status of brought forward losses/ allowances, if any.

26. Information for Review Period

- i. Copies of Return, computation of income, transfer pricing report (along with transfer pricing study) for three preceding years.

- ii. Copies of tax audit report and other annexure for the latest three assessment years.
- iii. Copies of intimations, assessment orders, submissions made, appellate orders etc for all open years.
- iv. Details of tax benefits claimed by the Company.
- v. Year-wise details of amount appearing under the heads 'provision for tax' and 'advance tax' as at March 31, 200_ and December 31, 200_.
- vi. Provisional computation of tax liability for the Financial Year 2000-, based on which the Company has paid advance tax instalments.
- vii. Computation of amount appearing as deferred tax asset/ liability as at December 31, 200_ and March 31, 200_.
- viii. Copies of legal opinions, if any, obtained by the Company.
- ix. Copies of wealth tax returns (along with all annexure) filed by the Company for three preceding years.

27. Indirect Taxes

Service Tax

Status of compliance and assessment

- i. Statement of domestic revenue streams and whether service tax charged. Verticals can provide details and sub-divisions thereof or chart on reasoned positions adopted regarding applicability of service tax.
- ii. ST-3 and credit returns filed.
- iii. Details of payments to foreign service providers for services rendered in India .

Challenges and Risks Covered in Due Diligence Process

- iv. Details of payments to road transporters.
- v. Details of all payments made to and services received from all foreign service providers.
- vi. Any audit objections received by the company after excise/service tax audit?
- vii. Agreements for services utilized and rendered by the company.

Customs

- i. List of goods, which are generally imported along with tariff classification and rate of duty.
- ii. Bills of Entry for all imports assessed provisionally.
- iii. Licenses granted (for import).
- iv. Licenses granted (under Duty Exemption Scheme).
- v. Status on discharge of export obligation and related documentation.
- vi. Status on discharge of legal undertaking/ bonds.
- vi. Status of show cause notices ("SCN") issued; submissions made, adjudication thereon and appeals.
- vii. Agreements pertaining to import of know how, technology, drawings, designs, etc.
- viii. Legal opinions obtained, if any.

Excise Duty

- i. Status of compliance and assessment.
- ii. Registration certificates.
- iii. Show cause notices, submissions made, adjudication orders and appeals.

Training Material on Internal Audit

- iv. Registers maintained for excise purposes including returns and credit returns.
- v. Documentation in support of credit and refund claims in relation to input duties/ taxes.
- vi. Outsourced job works/ relevant agreements for the same.
- vii. Exemptions claimed in the review period and those that are currently valid.
- viii. Legal opinions obtained, if any.

Sales Tax/VAT

- i. Status of compliance and assessment.
- ii. Assessment orders for last 3 assessed years (for CST, Local Sales Tax).
- iii. Returns filed during the last one – year.
- iv. Details of incentives claimed and periodical reports filed, if any.
- v. Details of declaration form pending receipt.
- vi. Classification determination order, if any.
- vii. Copies of all distribution agreement.
- viii. SCNs, communications form pending receipt.
- ix. Appeal petitions/ applications.
- x. Application for any sales tax exemption, along with related documentation.
- xi. Legal opinions obtained, if any.

ANNEXURE C

This specimen report attempts to cover venture finance, investment and a amalgam type transaction and it should not be construed as one intended for only merger and acquisition due diligence. The instructor may use this specimen report to explain the different aspects that a due diligence findings cover and its style of writing.

Sample Due Diligence Report for a Prospective Investment

This report is for the limited usage of the private party that commissioned it, and remains the property of the author. This report and its information is not for distribution, dissemination, or publication in any form or manner, including excerpts, quotations, summarisation, or paraphrasing, whether written, verbal, or otherwise. This may not be used by anyone, including the party that commissioned it, to persuade or dissuade other prospective investors.

1. Economics

In our limited review, we found some items of concern as reported in this section. These may or may not be indicative of problems, and should probably be followed-up with questions to the Company for clarification. We can pursue this further if desired.

- ◆ Evidence of high-end market - The Plan devotes considerable space to the general prevalence in the country of _____ problems, but shows essentially no data regarding the particular market for people who can afford to pay Rs. _____ to Rs. _____ (or more) out of personal funds to deal with it in a luxury setting. The presumed existence of such a sub-market is the cornerstone of the whole Plan. This target market may well exist to the point that four dozen such people can be found every month or two, for years to come, but no evidence is presented.

- ◆ Inadequate budget to provide deluxe environment - People that are paying this price range may expect private rooms, and better food and more personal attention than what is presently included in the Plan. People are to sleep two to a room, food is budgeted at about Rs._____ per month per person, and the professional staff is budgeted at about _____ professional(_____, etc.) for each five guests. Taking into account the 24/7 nature of the situation, the 1-to-5 ratio is actually even worse, at this would imply each guest would get about 1 hour per 24-hour day of individual attention, and actually less when further taking into account that some of the professionals' time will be spent in group activities, and thus unavailable for individual attention. Similarly, the Plan appears to provide for very few kitchen staff and housekeepers, especially in light of the 24/7 setting and the high-end clientele. There appears to be no budget for a _____, and a fulltime one would only allow an average of less than one hour per week per patient. It is the nature of most such start-up plans (i.e., for a new business model) to not anticipate all costs, and thus it would be both reasonable and prudent that a non-trivial allowance should also be provided for “Unanticipated Other Costs” (perhaps about 15% of the total of identified costs). These budgeting issues suggest lower profitability than what is indicated in the Plan, or worse, forthcoming client dissatisfaction with the experience, or, perhaps a lack of business/operational/management experience (and/or attention to detail) on the part of the founders.

- ◆ Significant omissions in the budget, or extra fees to the clients - The Plan states that “ all treatment services” as well as “outside functions” are included in the very large fee. The Plan describes a significant roster of “Adjunct Services” which will be available (e.g., _____services, management, _____- feedback, conditioning, _____, _____ treatment, _____ services, etc.), all to be provided by outside contractors. There does not appear to be any funds in the budget to cover this, which would likely be a significant cost. The alternative, of charging extra for these items, would not appear to fit well with the high-priced “all inclusive” portrayal.

Challenges and Risks Covered in Due Diligence Process

- ◆ Treatment pricing is twice as high - The Plan seems inconsistent as to the average cost per patient, variously citing full term price of Rs._____, a monthly fee of Rs._____ “an average length of stay of two months” (i.e., Rs._____), and Rs._____ per month in the PandL spreadsheet. Additionally, as above, will there be potentially substantial extra fees charged?
- ◆ Plan details for equipment and furnishings not provided - Perhaps it has been done and simply not included, but we see no list of major assets required, and associated costs of procurement, nor any estimate of the total funds budgeted. For example, the facility is in effect going to be operating a small restaurant, if it is to include all meals for 48 or so people (plus staff?), three times a day (plus late-night snacks available for the “deluxe” environment?), seven days a week.
- ◆ Financial results for the ramp-up years - The spreadsheet that we examined was not labeled as to what year it represented (i.e., the first year, or the fourth year, etc.), but showed the client load already at essentially full capacity. The economics of the ramp-up years were not shown in our copy; these years could possibly be more problematic in terms of cash flow.
- ◆ Higher density per building - The property is reported as _____acres with _____ existing homes, which are described as capable of housing 6 clients each. The Plan then provides for an additional -----homes to be built on the property, which implies they would have to house ten clients each to reach planned capacity; this larger group size is not mentioned.
- ◆ Competitive advantage - Being “first to market” (as stated in the Plan as a key competitive advantage) in this particular situation does not infer much in the way of lasting competitive advantage, as far as we can tell. Likewise, the Plan statement that their _____services... can not be duplicated” rings rather hollow. There is a strong market and few providers, these may not matter. We have not spent

time to search for possibly pre-existing high-end competitors; this can be pursued if desired.

2. Usage of Stock Sale Proceeds

In our limited review, we found items of very substantial concern in this section, which we believe should be clarified in writing with the Company prior to any investment.

- ◆ Document contradictions - There were two documents provided (“Confidential Private Placement Memorandum; Rs. 10,000,000; _____, Inc.; Equity Shares” and “_____ Confidential Document; Contact _____; _____, Inc.”), and these two documents at times appear to contradict each other, including with regard to the usage of share sale proceeds. It is our lay interpretation that the Private Placement Memorandum would be the definitive legally binding language; if this issue is a concern, an attorney should be consulted for a professional legal opinion on this issue (which we cannot and do not provide). For the sake of brevity, our comments with regard to the usage of proceeds apply primarily to the Private Placement Memorandum (“PPM”) document.
- ◆ Half of the proceeds to be raised are targeted to go to what is effectively the apparent anticipated cost of raising the funds. - This “half” also may well be the “first half”, i.e., if the full Rs.10 Million is not raised, the first funds (or perhaps even the first Rs. 5 Million) may go to these ends, leaving even less than half of what is ultimately raised for the business. This would appear excessive, and dangerous to the integrity of the stock investment from the investor's perspective. Of the other half, a significant piece is slated for overhead, analysis, and other “soft” costs; only Rs.4.2 Million of the Rs.10 Million is specifically slated for real estate costs, construction, and asset/equipment requisition. The PPM also states, with respect to the Rs.5 Million that is earmarked for the cost of raising funds, and all other categories, that “any unused sums in any of the above categories may be retained by the Company for any purposes ... including ... payments to the principals for management fees.” It is our

Challenges and Risks Covered in Due Diligence Process

interpretation, which may be incorrect, that the PPM states, in effect. That substantial amounts of the Offering may be paid directly to the principals, in unspecified ways, with no defined oversight or scrutiny.

- ◆ It is not all clear that the funds earmarked from this stock issuance will be used to purchase any property - The footnote that explains what the “Real Estate Costs” are does not mention the purchase of any property; rather, it says that this Rs.4 Million is “Reserved for the pre-payment and continuing of leases ...”. It further mentions “leasehold improvement for space renovations including architectural drawings and consultation.” This would appear to be a somewhat cryptic reference to the only lease mentioned, which is the presently leased _____, 000 square foot office space, which is not part of the residential property being considered for purchase. The PPM further states “The Company plans to use the capital provided by this Offering for advertising and marketing, accounts payable or other working capital and general corporate purposes that management determines are in the best interest of the Company.” We can find no place in the PPM where it indicates planned usage of the funds for acquisition of the real estate and facilities, which acquisition is the supposed cornerstone of the Plan. Additionally, it states “Management is not restricted in the application of the funds as provided in this Memorandum under the caption 'Use of Proceeds'.” This is close to a “blank check”. In our view, the charitable interpretation of these facts is that the PPM document is poorly written. We regard this as a substantial “red flag”.
- ◆ Stock investment could be at substantial risk if inadequate funds are raised in Offering - The Offering is being conducted on a “best efforts, no minimum basis,” stating that “There is no minimum amount of proceeds that must be raised before the Company may use the Proceeds of this Offering, ... The Company will have broad discretion in the use of these funds. In yet another area it states “Whereas the total amount of the offering may not be raised, there is substantial risk that if the total amount is not raised there may not be sufficient capital to complete any of the projects

contemplated. To that extent, the investor may lose all of the investment.” While it can certainly be claimed that this is “just legal boilerplate,” consider two things: 1) subscriptions such as this can be, and often are, structured such that if a certain threshold amount is not raised, then all the funds get returned; this PPM is very pointedly not that way; and, 2) the Company specifically states in the PPM that “The Company has not been represented by legal counsel in connection with the preparation of this Offering”. so who then wanted the deal structured this way, and that language included? If there is inadequate funding raised to accomplish the Plan objectives, the Company is under no obligation to return any funds to stockholders, and from all apparent writings, it would appear that the Company has no intention to return funds under such a scenario. This also plays in to a concern raised in Section 3 below.

3. Ownership, Control, Accountability and Investment Exit

In our limited review, we found items of very substantial concern in this section.

- ◆ *Present ownership and control:* At present, the majority of the Company's stock is reported by the Company to be owned by _ (35.1%), __ (19.2%), and _ (10.6%), collectively 64.9%, with the next largest holder reported at 7.4%. We have absolutely no further information on any of these people, including even what their first names are. They are not listed as Officers. The Board of Directors is not identified, and we do not know if it has even been established at this point. We do not have access at this time to the Articles of Incorporation, or the Bylaws, which could be critical. The PPM states that “certain provisions of the Company's Certificate of Incorporation and Bylaws and of ___ law may delay, defer, or prevent a change of control of the Company and may adversely affect the voting and other rights of the holders of Common Stock”.
- ◆ *Control by presently subscribing shareholders:* The Offering is for 10.0 million shares, and it states that there are

Challenges and Risks Covered in Due Diligence Process

presently only 0.2 million outstanding, and further, that the Company is authorised to issue a total of 25.0 million shares of equity stock, and that the Board can issue the remaining 14.8 million additional shares (subject to _____law) without stockholder approval. The bolders of these new shares (which could, or may have to be, issued at a vastly lower price) could then control the majority of the Company's stock. There is no mention that we saw in the PPM of any election of Directors shortly after the subscription for the present stock. The PPM states, "The Investors shall not be entitled to receive a copy of the list of Investors." It appears to us as a distinct possibility that unless someone (or a group of parties that knows each other before hand) subscribes to more than half of the current Offering, that the subscribers to the Offering may have absolutely no method of influencing the Board, even if 90% of the shareholders felt the same way.

- ◆ ***Accountability:*** near absolute power of the unidentified Board
 - The PPM states that if the Company has inadequate funds to carry on it's business, that it may issue more shares in a attempt to raise additional funds. The new shares may be of the same, or a different, "series" of stock. Further, the PPM states that the Board of Directors has the authority, without stockholder approval (subject to _____ law), to alter the rights, privileges, and voting of the shares outstanding (including those being offered in the PPM), and may apparently do so differently by series (e.g., to give the second series different rights than the first series). Lastly, the PPM states "the Board of Directors may authorize and issue Preferred Stock with voting or conversion rights that adversely affect the voting power or other rights of the holders of the Common Stock. In addition, the issuance of the Preference Shares may have the effect of deferring or preventing a change of control in the Company". This appears to be unconstrained by any stockholder vote. Our lay interpretation of this is that the common shareholders do not effectively control the Board here; this is not a legal opinion, and an attorney may not agree with out assessment. We see the combination of the items above as a substantive red flag.

- ◆ *Insulation of the Board:* The PPM states “The Company's Certificate of Incorporation and Bylaws contains provisions that limit the liability of directors ... and provides for indemnification of officers and directors under certain circumstances. Such provisions may discourage stockholders from bringing a lawsuit against directors for breaches of fiduciary duty and may also have the effect of reducing the likelihood of derivative litigation against directors and officers even though such action, if successful, might otherwise have benefited the Company's shareholders. In addition, a stockholder's investment in the Company may be adversely affected to the extent that costs of settlement and damage awards against the Company's officers and directors are paid by the Company pursuant to such provisions”. This kind of provision is not all that uncommon, and is sometimes used by bonafide companies to discourage frivolous lawsuits and to entice good people to serve as officers and directors; however, in conjunction with everything else here, it is worrisome. The PPM also states, “Investors shall not have the right to receive copies of any federal, state or local income tax or information returns. ... Investors shall not have access to the books and records of the Company”. Again, this may actually be not uncommon, but in our case, no independent outside auditors have been named, nor has there been any mention that some such chartered accountant firm shall be found; only annual reports are committed to (none quarterly, and nothing as to being audited).
- ◆ *Investment:* Substantial restrictions apply with respect to any sale of an investor's stock. Dividends are not assured, even if the Company is profitable. Prospective distributions to investors are not clearly defined. This is not necessary uncommon.

4. Founders, Officers, Principals

In our limited review, this section came up largely neutral. There are a couple of things that would be problematic if they are truly associated with the Principals; we can pursue this further if desired.

Challenges and Risks Covered in Due Diligence Process

- ◆ *Same level of comfort established* - In the time allocated for this section, we did not find any conclusive evidence that any of the principals identified have problematic records. It should be noted that this is not always easy to find, and we did not, for example, spend the time yet to check non-current records. We have not done thorough background checks. We have, however, done enough probing to give us some degree of comfort with respect to the principals. We spent a fair amount of time looking and coming up with nothing, which in general is a good indication. If thorough background checks are desired, please let us know.

_____ appears to be bona fide. The proposed Chief _____ Officer, _____, is shown on the website of _____, as the Director of the _____ Centre, where it states that he “has more than 10 years of experience in _____” and that he “received his _____ degree from the University of _____, _____ School and has practiced _____ for 15 years,” among other things.

- ◆ *No certain information found on other* - There was no definitive information of any sort (positive or negative) found regarding _____ (the proposed CEO), or _____ (the President), _____ state corporation records show Mr. _____ as the only listed officer, holding positions of President, Treasurer, and Secretary, and listing a _____ address from him. We likewise found nothing on the two or three largest present shareholders; their last names are somewhat common, and only their first initial is listed (a with no indication of where they reside), so it is not likely that anything conclusive would be found on these names, even if it certainly exists. We have no indication at this point if these shareholders are insiders or exert any real control or influence.
- ◆ *Potential problem areas* - There were several pieces of non-conclusive information, which may well be coincidences that do not pertain to the principals; however, if they did actually pertain, it would be of significance, and troubling. These can be investigated further if desired. They include two of the companies listed in the experience portion of Mr. _____'s bio-data (where he was alternately the _____ manager and

the CEO) are not listed with complete names (i.e. "ABCD" and "T.S.G."); there is (or was) a company called "PMFG" of PQRS City, California that has had troubles with the SEBI; likewise there is a "TSG" that has also had troubles with the SEBI. It would be prudent to simply clarify the complete names of the companies that Mr. _____ worked _____ for. Additionally, there appears to be another, different, _____ on the west coast in the same field; there is _____, Advanced _____ Care" website, with a different educational and professional background; the site also has a photo, at www. _____ . com. We did not call to check Mr. _____'s prior employment claims.

- ◆ *Corporate identity* - The Company was incorporated Sept. _____200_____. The Company has a website domain name reserved at www. _____--. Com (with no functioning website yet). There are at least two previously existing organisations with similar names.: the _____ at _____ the University of _____ is sometimes referred to as the _____. There is a _____ in _____, _____(which may be near _____).
- ◆ *Officer's stock* - The present officers appear to own no company stock at present, although there are _____ shares variously described as either "reserved for management" or "owned by officers and directors" (although there are only _____ shares listed as having been issued to date, and none of these shares are ascribed to any of the listed officers).

Company's Officers and Directors may beneficially own a significant portion of the outstanding equity Shares of the Company."

- ◆ *Officers' compensation* - There is conflicting information regarding the proposed compensation of the officers. The PPM states that "All compensation to the Company's Executives will be in the form of stock and/or stock options for the foreseeable future." On the same page it also says "Officers and Directors are expected to draw limited salaries after this Offering has been successful." Note that it is generally not common that directors would immediately

receive salaries in the initial stages of a start-up, and that the identities of the Directors has not been provided, nor has anything been established with regard to elections of Directors; so who then are the Directors loyal to? The shareholders, or the people that pay (and determine) their salaries? The PPM further states, "For the most part, these persons control, and will continue to control, their levels of executive compensation in future years, which may be significantly higher..." The spreadsheet attached to the other document (not the PPM), shows Mr. ____ with a Rs. ____ per year salary, and a bonus (not necessarily all to him) to be paid of another Rs. _____. While talent should be paid well, and if this is successful such compensation may not be at all out of line, this comes across to us as being handled in a less than forthright manner. Nothing is shown with regard to compensation plans for Mr. _____, who is the only officer listed in corporate records, and who is President and Treasurer, and is not listed as a shareholder in the PPM. Mr. _____ is presumably not doing this for charity, and the complete lack of any disclosure regarding his financial ties adds to the overall problematic lone here.

5. Summary Conclusion

We believe that either this has been inadvertently poorly written and structured, or else it is a rip-off. It is difficult to tell which, even if it is not inadvertent, it is likely that some of the principals may be entirely innocent, such as Dr. _____ who may have been talked into joining this, and may not be involved in or knowledgeable about the structuring, financial, and business issues. In either case, we would not be comfortable recommending it unless certain aspects of the Offering were changed, and some additional disclosure was made. There are some important issues here (as well as a number of possibly not so important ones). Some of the key ones may largely be legalistic "technicalities" but they could absolutely be deadly to an investor, and they are in cumulative total, "out-of-line". If they are not intended, they should be changed.

The investor is, in effect, depending entirely upon the goodwill of the Board of Directors in order to not be screwed, and the Board

Training Material on Internal Audit

is neither identified nor is near-term elections plainly provided-for. Important items to consider include:

- This Company has been set-up to largely bypass the normal accountability and checks-and-balances. Perhaps they do not intend to utilise that capability; are you comfortable in counting on that?
- It does not appear that they are bound to use any of the proceeds raised to actually acquire the necessary real estate.
- It appears that if the Offering is less than fully subscribed, then there is significant possibility that the subscribers will lose their entire investment.
- It appears that a huge portion of proceeds raised will be paid to people raising the money, and very possibly to the founders.
- Additionally, there are potentially significant documents not disclosed, and the budgeting appears amateurish.

Chapter-VII.5

Introduction on Fraud and Investigation

Fraud encompasses a wide range of intentional acts leading to any kind of damage to an organisation. It may be noted that the damage need not be financial only. It impose greater difficulties in detection than errors, since there is a significant difference between frauds and errors; errors are a result of inefficiency or oversight, whereas frauds are the result of shrewd and efficient planning. Errors are inadvertently committed *without any intention of concealment*.

Frauds are of such vicissitude and have far reaching effects that it would be unthinkable to describe every type or even all *major* situations of fraud. However certain common situations, in which internal auditor are likely to find themselves, have been envisaged and briefly described below:

Conventional Investigation Assignments

The management may ask the internal auditors to extend their audit to apply such extended or modified procedures as may be necessary to assess, evaluate and determine the nature and extent of fraud. This kind of assignment is a regular investigation and needs no elaboration. Such investigations could cover cash embezzlements, asset losses, revenue leakages through inflated or replicated invoices, suppression of income, inflation of liabilities, deflation of receivables and the list could go on and on.

Bank Frauds

This area has the highest potential of fraud. The raw material in banking industry is money itself. Frauds can be perpetrated within a bank itself or by outsiders. Insiders may manipulate funds, loans, and apply teeming and lading between favoured accounts.

Outsiders could defraud a bank by furnishing fabricated, duplicated or altered demand drafts, cheques, bills of exchange, and other negotiable instruments. Apart from these, borrowers also often cheat banks in hypothecation agreements by inflating inventories or even providing substandard or spurious stocks with little or no value. Internal Auditor may find their role as investigators or a part of the inspection team. These days even pre-facility audits are asked to be carried out. These are audits in the garb of investigations to ensure that funds are going into safe and reliable hands.

Business risk Evaluation

This is another area of professional opportunity for internal auditor . Every business venture is always fraught with risks. What varies is the degree and the extent of the risk. Take, for example, a case where a company which want to go for the expansion requires a huge finance say Rs. 100 crores. In such a case his service can be taken to inquire into the feasibility of the scheme as well as the reliability of the finance provider. Further more he can be called tie evaluate bottom line if they goes for the a new vendor, or a new client or a new venture in the near future.

Insurance Claim Frauds

Claims for loss of stocks and loss of profits of large values, particularly exceeding Rs. 5 crores are usually surveyed in detail with professional help by most insurance companies. More often than not these claims are inflated, with or without intention. In such situations as well, internal auditors are being called to review, inquire and investigate into frauds.

Compliance Verifications

There are so many situations where specific guidelines or directives have been laid down for the use of funds. For example, a large trust may be given a donation of Rs. 10 crores for a project, say, providing for orphans and widows. The donor may want an assurance that the funds donated have been

Introduction on Fraud and Investigation

appropriately used. It is possible that this could turn out to be a thriving ground for frauds and misappropriation of funds. Similarly a hospital may have been given funds for a specific ward with conditions. There could be misrepresentations and false reports. A business may have a remote site where certain activities may be in progress. A possibility of misuse of resources is also likely.

In all such situations, internal auditor provide a cense of assurance that the fraudulent activities are not been indulged with.

Types of Frauds and Financial Crimes

An Internal Auditor may be well advised to study and understand certain types of frauds and manipulations which he is likely to come across. The situation and technology applied might differ in each case, but the core nature of the frauds will be the same. The following are some of the typical frauds which an examiner needs to understand:

Trojan Horse Frauds

The name is derived from the Greek mythology of the Trojan Horse where the Greeks could not break through the Trojan defence and they created an innocent looking wooden horse to test the Trojans. The frauds which are committed in two phases.

- The first phase is that during which the resilience and strength of a control is tested by the potential fraudster.
- The second phase is then activated during which the actual act of damage is undertaken after the fraudster is satisfied that the critical period has passed and that he can go ahead with a minimum of risk.

Note : If the fraudster is effectively pass through the first phase then it go to the second phase else will not proceed further.

These frauds are perpetrated with considerable planning behind them and an astute mind masterminding them. The most effective preventive steps that could be taken are:

- (a) identify key controls in every system and
- (b) to constantly test key controls.

The testing of key controls, using tiger teams testing could be effective. In this test various conditions are artificially created and the system is tested practically. Conditions under which the controls do not work or levels at which procedures wilt under pressure are then examined for possible remedial and corrective measures. This increases the management preparedness and it weakens the confidence and reduces the safety level for perpetration of a fraud.

Disaster Frauds

These are frauds which thrive on situations of disaster, chaos, anarchy, and disorder. The fraudsters operate under the shield of the confusion created in such situations. In the event of a calamity such as fire, floods, earthquakes and other accidents, naturally the organisation is reeling from the aftermath and shock. It becomes impractical or impossible to comply with systems and procedures and information and evidence can be easily suppressed. Knowledge of asset location and whereabouts, weaknesses and strengths of controls and access to other sensitive information can be used or misused. Assets, valuables and information can be stolen, sold, damaged or destroyed for ulterior purposes. Just as a patient recovering from an accident has to be extremely careful to avoid catching a dangerous infection, so also an organisation has to be very cautious while trying to stabilize itself after a disaster. *Take the case of a warehouse keeper who was in a warehouse where there was a huge fire. There were stocks of electronic items such as calculators, memory chips, and other items which were lost by fire. By the time the fire could engulf the entire warehouse, some stocks could be salvaged. However the insured might not have disclosed any or all of the stocks salvaged to the insurance company.* That is why every insurance claim has to be carefully scrutinised and examined from several angles to ensure that all clues fit in satisfactorily. It is dreadfully simple for a claimant to inflate the claim and later explain it away as an error if caught. The insured also has the convenience of stating that all records are lost or are in a disarray and cannot be retrieved.

These kind of disaster frauds are the relatively simple ones, but there can be more malicious ones also. There could be case where the disaster is created to shield the fraud like a *classic case*

of a loss making hotel in a remote location where a new manager was able to show profits. There was a sudden turnaround and the hotel started making astronomical profits even though business conditions were gloomy and room occupancy had not perceptibly gone up. Amazingly, the profits were evidenced through full cash receipts; therefore there was no room for doubt in the minds of the management. However what was really happening was that the manager was selling off expensive assets of the hotel such as chandeliers, paintings, cut glass show pieces, etc. Elegant teakwood furniture was replaced by commercial plywood furniture. Part of the money was routed back to the hotel as sale proceeds to show an upswing in the business and gain the confidence of the management, and part of the money was pocketed. When the hotel was fully stripped of all its resources, the manager decided to set it on fire to escape accountability and hide his fraud. Such a fraud is far more serious and affects the organisations' financial position, goodwill and can attract even statutory liabilities. One of the most effective methods is to evaluate the sheer logistics of a situation.

Achilles Heel Frauds

Such an approach was named after the legendary Achilles who was who was invincible but for his heel. Thus the fraudster look for the weakest point in the system and try to capitalised on the same. For Example, *a company had newly acquired an accounting system. As in every accounting system, there were several input documents, each of which had several fields for information. The management had bought the software off-the-shelf, on recommendation of a professional, and had not paid much attention to its minute details. However the accountant did, and found that the module for receipts had two fields for dates: the date of 'receipt' of a cheque and the actual date of the cheque called the date of the 'instrument'. For example a cheque may be prepared by a debtor on say November one (date of the instrument), but may reach the creditor by post only on the fifth of November. The software provided input of both dates to facilitate analysis of collections and corresponding entries in the records. The management was blissfully unaware that the accountant was entering the instrument date in the system to clear a favoured debtor's account. Accordingly the debtor was given a credit*

retrospectively for a payment made even a month late, merely by dating his cheque a month earlier than the date of its delivery. This entitled the debtor to get all bonuses and the early bird incentives which he shared with the accountant. Such small little items often are inconspicuous but could have incredible impact. In the above case where the company had a panel of 1000 debtors, the fraud damaged the company's working capital to an average of almost Rs. 20 lacs per month. To curb such a fraud system testing is essential not only at the beginning but also for some time during actual implementation to learn, understand and combat flaws which surface only on practical usage.

4. Corporate Espionage

*Today, information carries the highest value and frauds which sell information about a company to its competitors are on the rise and considerable time and money is being spent on this by large corporate houses. **Such frauds are almost impossible to prevent and deter.** For one thing, information is intangible and cannot be missed such as a pilfered asset or money. Secondly, facilities for transporting it through e-mail, internet etc, are easily available. This makes it even more impractical to monitor misuse or theft of information. No amount of security will completely prevent a fraud. The only thing that can be done is to minimise damage. This can be partially achieved by applying the '**red herring method**'. Use of decoy storage is found to be very effective. Keep sensitive information in two or three places, *of which only one has the full correct information*. The chances of the correct information leaking out are that way reduced to one-third. This must be supplemented with constant patrolling of all priority systems to see that there are no security breaches and violations, however small, insignificant or accidental they may seem to be. As even accidents must be examined for causes and sinister possibilities. Non-compliance of security rules must be viewed very seriously to enforce discipline. Lastly, special training sessions must be held to educate employees at all levels as to the dangers of such corporate espionage activities, the company's policies, and penal action.*

Technical Frauds

These are frauds which can happen right in front of the eyes of the management and it may not even know that it has been defrauded. This is because technical aspects are beyond the comprehension and frauds using these as a cover, are difficult, if not impossible to detect. *A fraud of a high magnitude was observed in a case in which a plastic component manufacturing company used the services of external vendors possessing moulds for manufacture of such components. The raw material was sent to the vendors (moulders) to process and return the components on the basis of norms fixed in advance. Apparently, the vendor was giving a good yield for the material sent and the company had no reason to complain. However in reality, the vendor was not utilising the raw material fully. About 90 % of the raw material received was mixed with scrap and processed. The balance 10 % unused raw material, was used for personal consumption or sold outside and the proceeds pocketed. Since the volumes of production were high, even a mere 10 % scrap mixed amounted to a raw material saving equivalent to Rs. 25 lacs annually. The quality control division of the company did not possess sufficiently sophisticated tools to evaluate the quality of components produced. The norms for input- output ratios had not been revised for a long time. The vendors also kept the quality control inspectors happy so as to ensure a smooth approval and acceptance of processed material. Such frauds can happen in any kind of company when it doesn't have the appropriate quality assurance mechanism*

Chapter-VII.7

Red Flags in Detection of Frauds

In fraud detection jargon the term red flag' is commonly used. As obvious red flags are nothing but symptoms or indicators of situations of frauds. The following are some of the red flags which examiners are likely to come across and understand.

Absence of rotation

Absence of rotation of duties/ activities prolonged exposure in the same area could lead to indulgence of the fraud hence, it is very well required that the appropriate personal or as we see in the technical frauds example it could be checked through the proper quality assurance practice and moreover, through the development of the new job worker or even follow of the industrial standard norms.

Close nexus with vendors, clients, or external parties

There would be a conflict of interests if an employee, particularly at a senior level, were to have close relations with a client. For example if a loan officer were to go on a Caribbean cruise with a borrower, it is quite likely that his friendship might come in the way of his duties regarding the loan monitoring obligations. The independence of a person can be evident from the manner in which he behaves with external parties.

Sudden losses

A company doing quite well suddenly makes huge losses. While there could be genuine reasons, mismanagement of funds and resources are more likely. These losses are likely to have been there all along simmering under window dressed accounts. Once the bubble bursts, however the losses erupt and it appears as though sudden losses have hit the business. These genesis of the

losses could have been systematic siphoning of funds, by inflation of expense or suppression of income or a combination of both.

Too Good To Be True (TGTBT) syndrome

This indicates that lovely glossy report may be furnished whereas in real terms there are gloomy conditions. For example an *EDP manager was apparently a very dedicated man. He would be the first to enter the office and usually the last to leave. He was highly respected. But what an investigation later revealed was that he was involved in manipulating data and certain in-house applications for receivables and payables to transfer credits to certain favoured parties. In fact he was manipulating his own loan account to show nil overdue even though he had not paid for several months.* The point here is that what appears to be good needs to be tested before accepting the truth value.

Generation of 'orphan' funds

Funds which are held in a fiduciary capacity and for which there is no accountability are thriving places for frauds. *Funds collected by trusts or donations in cash collection boxes are typical examples where there is no accountability on either side.* Neither does the donor concern himself about the usage of the funds nor does the beneficiary have a direct claim or even awareness in respect of such funds. However such funds can be substantial and invite perpetrators of fraud. Thus such situations are the places where any investigator must look into first.

Disaster situations

Accidents where books have been lost, or damaged, or catastrophes such as fire, earthquake, floods etc are other places where fraudsters can feast. The conditions offer ideal camouflaging conditions as explained in paragraph 2 earlier in chapter II.

Missing documentation

This is the surest sign of fraud and practically every situation of missing records either has been created to suppress a fraud or if

such a situation happens to emerge, it is used to engineer a fraud. For example, some records have been stolen or lost during shifting of an office. Deliberately the list of records lost could have additional missing items to provide for a future defence against ulterior motives. The larger the organisation the greater the chances of losing or misplacing records. Opportunities to palm off frauds by mysteriously disappearing records are easy and galore. Therefore missing documentation is a very strong signal of possibilities of fraud.

Chaotic conditions

As a corollary of disaster situations, conditions where accounts are in arrears, messy state or unreconciled, by and large are artificially created. The reason given normally is shortage of staff or resources, but this is more of an excuse. In several such situations it was found that there was no assertive effort to increase or ration the available resources. The shortage was artificial and an optical illusion to allow this disorderly state of affairs which in turn wonderfully camouflaged secret and evil designs.

Irrational behaviour

Behaviour which is not becoming of the employees' position and which does not keep in mind the decorum of an office often stems from deep rooted insecurity which could be symptomatic of fraudulent intentions. For example, a person who is always rude and inconsiderate, or overly secretive, is likely to be behaving in that way to suppress fraud or some kind of deceitful act. The intention is to keep others at bay so as to avoid inadvertently revealing guilt or to cover some malafide act.

How A Checklist can Include Certain Questions to Indicate Possible Red Flags?

As explained above, red flags are anomalies or 'Clues don't fit' situations. As stated earlier there cannot be and should not ever be a standardised fraud detection checklist. Yes what can be used is a common checklist which must be *adapted* and customised to a given situation using one's skill and judgement, and in

consonance with the existing set of controls and deficiencies noticed. When one reviews a system whether as an auditor or investigator or a chartered accountant in any role to detect fraud, the usual audit checklist can always be an important component. A few additional focussed questions and other checks explained later need to be added at the right place so as to reveal fraudulent motives. There were several aspects of concern such as extremely high volumes to one vendor, absence of sophisticated tools, close relations between vendor and the quality control managers. A checklist could have been added to the usual audit checklist, so as to focus it on the fraud suspected as follows:

- a) Are the supplier and the Quality control manager too friendly? If so, how can one find out? Check statistical data for a reasonably long period for granting approvals; how many times have queries been raised? What are the kind of queries and what has been the supplier's response? *(This data will provide some evidence of the close ties, if any, between the two).*
- b) How many times has the supplier actually issued credit notes for rejections and what is the percentage in comparison with the volume of business?
- c) Is there any resistance from any quarters for empanelling new vendors? *(The resistance could be covert or indirect; such as vague inquiries with unreputed parties so as to put the existing supplier in a good light. The existing supplier will always be depicted as the best choice by highlighting all his strengths and all the weaknesses of the proposed new vendors).*
- d) Does the existing supplier appear to be charging very reasonable rates, particularly in comparison with other suppliers? If so, this is one of the surest signs of something afoot. Most such cases are those where quality considerations are compromised. Nobody is a good samaritan and there is no charity in business. If a vendor is supplying, apparently at a rate which appears to be amazingly low, 9 out of 10 chances are that he is taking advantage in some other way.

- e) Verify stocks at vendors and reconcile balances of material with them regularly, and if possible, even on a surprise basis.
- f) Observation of a production cycle could also furnish incredible results particularly in respect of rejection percentages. Very often companies have a norm for rejections and wastages and scrap. These can change on account of environmental changes, technology improvements etc. Vendors can make tremendous profits by suppressing the actual rejection percentages.

Thus what is shown above is a typical investigation or fraud detection checklist. There is no limit to imagination and the best guidance in compiling a check list is experience.

Chapter-VII.8

Steps in Conducting an Investigation

Fraud detection assignments are unique and peculiar to the environment and the organisation culture. Therefore these steps should best be viewed as various options which may be applied individually or collectively. All of them may or may not be necessary in every case as it has a linkage with the objective of the assignment and the kind of information so desire.

Defining the Specific Objective of The Fraud Detection Assignment

The Objective of the Fraud Determination can be describe through the Internal Audit Charter so laid with the management . Following are some of the illustrations of an objective of a fraud detection assignment:

- Determination of a reason for a drop in profits in a particular branch where several allegations of corruption and mismanagement have been received.
- An investigation into shortage of inventory or cash, pointed out in an audit report as to the extent of shortage, the procedural control deficiency, and the perpetrators involved.
- A general risk management exercise in a company initiated by an audit committee with a specific emphasis on fraud detection.
- An investigation into a borrower's slow-moving loan repayment coupled with an adverse inspection report pointing out substandard or spurious hypothecated stocks at his godown.

- A covert inquiry into the activities of a purchase manager who had suddenly amassed substantial wealth from apparently limited sources. A suspicion of vendor corruption and unhealthy activities to be confirmed or dispelled.

Finalising the Terms of Reference with the Appointing Authority

It is vital to clarify and remove all doubts as to the real motive, purpose and utility of the assignment. The internal auditor should keep following considerations in mind:

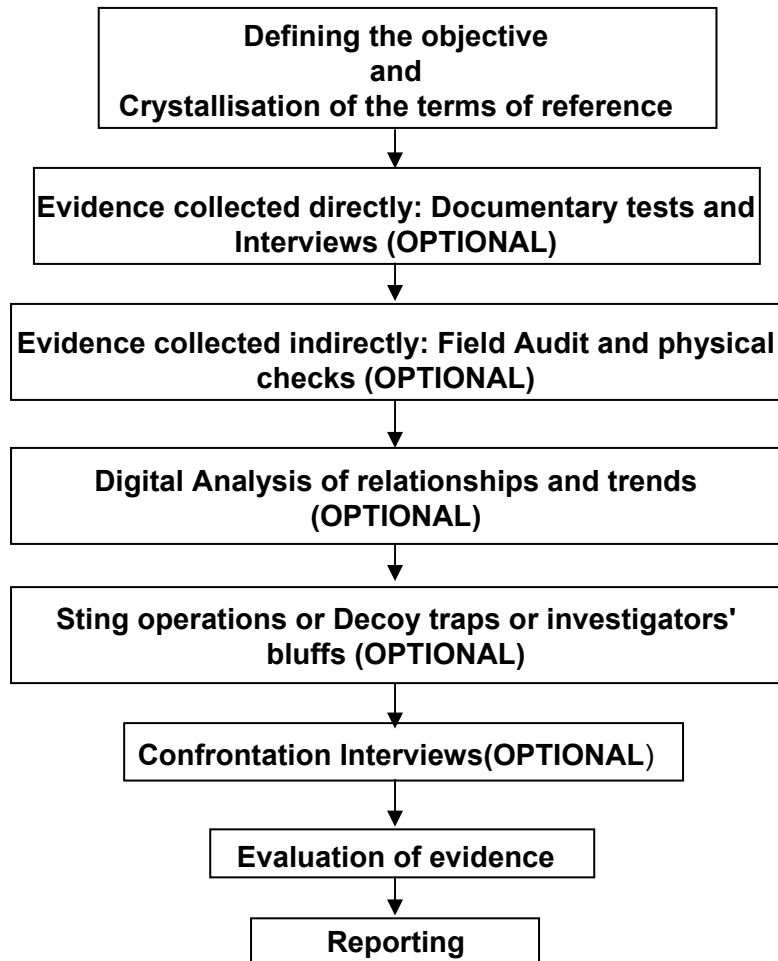
- *Motive and Utility*: Fraud detection, unless it is initiated under some statutory provision, needs absolute clarity of thought, motive and its utility. What is the report going to be used for? Is to assess risk merely or to find out whether a particular kind of wrongdoing exists or whether an allegation is true? This understanding will facilitate the examiner to undertake and conduct the assignment meaningfully. In order to leverage its utility to the maximum, it would be desirable to understand the nature and background of the *authority* to whom it is reported.
- *Materiality levels*: Determine also what is the level of *materiality* in consultation of the management. This is essential because some degree of fraud is present in every organisation. Some organisations even have a philosophy of allowing and accepting *some* leakage as a necessary business expediency cost. That level should be clearly understood so that the investigator does not cut a sorry figure in the end by detecting something which is immaterial. What may be serious to one organisation may be immaterial or insignificant to another.
- *Authority vested in the examiner*: The examiner must also clarify the extent of his authority in gathering evidence, examining documents, interviewing internal or external people, consent to use recording devices or other methods for gathering evidence. Thus these assignments are very customised and require tremendous contemplation at the initial stages. Ideally the terms of reference must identify the

scope of work and the extent of authority presumed in gathering evidence.

- *Confidentiality and reporting obligations:* The levels at which matters need to be discussed and represented must be known so that the examiner does not inadvertently reveal any management strategy or information about the assignment. It would be very useful to obtain a list of employees who can be approached for assistance. Similarly, the authority to whom the report has to be issued should be identified and spelt out. This will avoid embarrassment if someone at a lower level asks for a report. This is important so that there is no ambiguity as regards the issue and usage of the report. For example an appointment for an investigation may have to be reported to a parent company overseas and not to a local company in India. This must be specified at the beginning.
- *Spelling out constraints or impediments: expected based on the above or the experience in the past:* If there are any constraints of time, resources, non availability of records they must be spelt out in advance. The constraints could also be in the role of the examiner. Seven out of ten cases, where fraud is suspected, will specify that the examiner carries out his assignment covertly. To illustrate, the examiner will be asked to pose as a system consultant, or an internal auditor, or an accountant or someone other than an investigator. If such conditions are laid down, the terms of reference must specify that findings will be subject to such constraints which will impede access to information and evidence due to the covert nature of the assignment.

Chapter-VII.9

Various Steps Which can be Considered in A Situation of Fraud Detection



Note : Any of all the optional steps could be applied, and the sequence of the steps may change in a given situation. Further a particular step could be attempted more than once also.

Direct Evidence Collection: Documents and Interviews

The actual work commences by searching for information or evidence through *direct* channels. Direct channels would be those which are directly available in terms of records, documents and information from the organisation's internal sources itself. The examiner also has to understand and appreciate the internal environment to ascertain whether there are factors which reduce or enhance the possibilities for perpetration of fraud. This requires appraisal of control systems, procedures and level of documentation. This is done through appropriate documentary checks and tests. As regards examination of records and documents, much of what is done at this stage is similar to the systems and procedural check done during audit function. The difference is in the focus and the depth of the inquiry, the method of gathering information, the tools and techniques applied, and the maintenance of working papers. Auditors would generally accept records and documents at face value, unless something unusual is noticed. For example, if there is a signature according approval on a document, an auditor would accept it. However in fraud detection an auditor would keep specimen signatures of the sanctioning authorities so as to enable him to spot possibly forged signatures. Fraud detection may even use services of experts much more than an auditor would. In fact several fraud examiners have a team which include handwriting experts, interviewers, field investigators surveillance experts and others who would be useful. The exercise would embody even the conventional audit procedures but in a much more detailed manner. This would be a focussed and concentrated audit with a sample substantially larger and more comprehensive and fine-tuned to meet the requirements of the situation. For example, if it is suspected that the purchase manager is favouring a particular vendor, then all inward challans, purchase invoices, purchase orders relating to *that* vendor may be examined. Perhaps all transactions initiated by that purchase manager may be scrutinised also. This is done with the simple objective of gathering relevant and *meaningful* information with reference to the objective. The documentary tests are supplemented with information and explanations obtained through preliminary interviews of all those employees who are deployed in

the area being examined. Documentation of this is of paramount importance. Cases of people changing statements at a later stage on account of new evidence being revealed are not uncommon. Therefore it may be worthwhile using tools such as recorders, explained in a subsequent chapter, to have submissions on record at every stage.

Indirect Evidence Collection: Field Audit and Physical Steps

Every fraud detection exercise usually encapsulates certain field verifications. What are field audits? These are verifications *external* to the organisation, in addition to the book keeping and documentation checks and tests carried out internally. Field checks are carried out to ascertain, or corroborate, or supplement information or evidence obtained from the direct sources. The conventional audit procedures of physical verifications of cash and inventory are a typical example. However this is merely one of the many categories of field checks. There can be an unimaginable variety of field checks peculiar to a situation. Some of the examples are given below:

- Field audit of payroll disbursements to unearth 'phantom' or ghost workers. Verification of existence of all employees or workers with reference to names appearing in a payroll. There have been cases detected where non existent workers have come to light by auditors or investigators being present and observing actual disbursement of wages.
- Field verification of vendors' offices to detect non existent suppliers at the places or addresses given on bills. If they do not exist the chances are that the relevant bills are fictitious. For example purchase of stationery from a supplier who does not have an office at the address mentioned could mean that fictitious bills for stationery supplies have been inserted into the system.
- Physical verification of cash, stocks, fixed assets, investments as represented in the books of account. This principle may need to be extended to such assets lying with

third parties also. Verification could also be for expenses incurred. For example construction or even repair costs of a boundary wall could also be physically verified for falsification of any kind.

- Technical evaluation of assets or stocks. Physical verification is one aspect which merely proves existence of something stated in the records. A technical evaluation provides assurance or reasonable support in terms of the nature and value of the asset as represented in the records. For example purchase of a computer with a specific configuration can be confirmed by someone technically qualified to ensure that the configuration paid for exists physically on the system.
- Verification of accounts, with third parties at their offices or sites. There was a very interesting case where the balance confirmations with a party were matched perfectly. Therefore the auditors did not see anything dubious. However an exercise of reconciliation of the statement at the party's office revealed that the party's ledger had lesser number of transactions. *An investigation revealed that since this was a very old and trusted party, and since there was a phenomenally large volume of bills received from him, usually his bills were not scrutinised nor questioned in detail. Fictitious bills were presented and paid but those cheques were cashed clandestinely in a bank account specially opened with an identical name. These transactions were easily camouflaged in the large volume of this party's transactions.*

Digital Analysis of Relationships and Trends

Further, an analytical review of percentage checks for comparison of transactions with other similar vendors may also be done. *These provide additional shape and direction to the observations made so far.* Analysis has to be done to establish existence of relationships or to throw out anomalies which could further provide evidence of wrong doings. Digital analysis may be done for

financial or non financial data. Financial data analysis includes management ratios, debtors' and creditors' ages, marginal costing and budgetary variances are all barometers of financial discipline. However non financial data can also provide a wealth of information. For example:

- A comparison of the average number of days taken to approve a particular vendor's bills or to issue his cheques with the average number of days for the approval or issue of cheques to similar other vendor / s could substantiate vendor kickbacks or a nexus between the vendor and someone in the purchase or accounts department.
- A trend examination of orders placed with a particular vendor over a period could indicate results which could confirm suspicions about over friendly relations with a specific vendor e.g. excess ordering above requirements may be an indicator of favours granted.

It would be advisable for any fraud examiner to archive all relationships of such non financial data into a kind of a checklist for future assignments. This will facilitate making evaluations of a phenomenal kind with incredible results.

Sting Operations, Investigators' Bluffs or Decoy Traps

A sting operation or an investigator's bluff or a decoy trap is a procedure of trapping a suspected perpetrator of any wrongdoing in the act. THIS PROVIDES DIRECT EVIDENCE, DIFFICULT TO REFUTE. In common terms, it means laying a trap to catch a crook or thief red handed, a kind of a mouse trap. This also forms a part of some fraud detection assignments because certain frauds are otherwise difficult to prove. The following illustration proves this point.

In a trading concern dealing in chocolates and sweets having a chain of stores in all the metro cities, the management decided to have an incentive scheme to induce shoppers to visit their shops again. The scheme required shoppers to make a purchase of more than Rs.

1,000 to entitle them to get a 10 % discount coupon for their next visit. A placard was to be prominently displayed at each of the shops to bring about awareness of the scheme. Appropriate internal controls in the form of serial control over receipt books, and discount coupons were introduced also. The auditor carried out a usual audit plan covering sales, purchases, cash and bank transactions, salaries, and journal entries, using appropriate statistical samples. He did not notice anything untoward and the financial statements and the books of account seemed to be in order. The serial controls, Cash totals, cash registers all tied up satisfactorily. However, there was one small anomaly. In one of the metro cities, consequent to the introduction of the scheme, the sales had not increased, though large value of discounts had been availed of! All the other metros showed an upswing in consonance with the budgets. Even the management was intrigued by this result. The auditor was asked to investigate. The auditor decided to apply a field check by visiting that metro. On a personal visit, the first thing he noticed was that the placard regarding the Scheme was not displayed. Obviously, shoppers could have had no other way of knowing whether such a scheme was in force unless the cashier was, as a matter of routine, informing shoppers purchasing chocolates worth Rs. 1,000 or more, of the discount entitlement and furnishing discount coupons. He went through all the past discount coupons encashed by customers and found that most of the shoppers who had purchased chocolates and sweets over Rs. 1,000 had purchased chocolates or sweets worth much more on the next visit. Even more intriguing was the fact that a lot of shoppers had visited the shop again on the same or the very next day to purchase chocolates. This was unusual because normally chocolates are not 'stocked' and a shopper would generally buy his required quantity on the first visit itself. This led the auditor to believe that the discounts were not genuine. However, since the names and addresses of the shoppers were not available proving any foul play was difficult. This was an ideal place to try

the sting operation or an investigator's bluff technique. He decided to test out the scheme, by planting a shopper who purchased chocolates worth Rs. 2,500. As expected, the shopper did not get the discount coupon. He was given a receipt of Rs. 2,500, numbered 20026. The receipt had left the spaces relating to information of discount coupon, as well as the net payment amount blank. At the end of the day, the cashier reported his total cash sales for the day and a statement of discount coupons issued, which showed that discount coupon no 2113 had been issued against the receipt 20026. The auditor immediately confronted the cashier who confessed that he had fraudulently retained the discount coupon himself. He explained how he was cashing such discount coupons as follows:

- Step 1: Receipt 20026 was issued to A for Rs. 2,500/-*
- Step 2: Daily Cash Receipt and Discount coupons statement would disclose:*
- Coupon 2113 against Receipt 20026*
- Discount Coupon 2113 was actually in possession of the cashier.*
- Step 3: The cashier awaits another customer purchasing chocolates who does not ask for a receipt. The cashier would make out a receipt for the value of purchase which was say Rs. 1,500/- and append the discount coupon 2113 for 10 %, indicating a deduction of Rs. 150/- in the discount column.*
- Step 4: The cashier would pocket Rs. 150/- and place Rs. 1,350/- in the cash box.*

In this manner he had siphoned off almost Rs. 20,000 per week. This would never have come to light if the auditor had not applied a field check, and followed it up with the sting operation. Very often the audit procedures applied by the auditors do disclose weakness in controls and anomalies in findings. However, the

audit falls short of discovering or bringing to light the actual damage done and the nature of deceit or trickery. It is therefore essential for him to recommend to the management to use such fact finding techniques to determine whether control procedures are being implemented. That is also why personal inspection, visits and 'walk through tests' are very meaningful where situations so demand an 'investigator's bluff as shown above can be effective.

Exit Interviews or Confrontation Interviews

Where doubts and suspicions regarding existence of fraud are dispelled, a list of reasons for so concluding are prepared and the management may be reassured that there is no cause for concern. If unfortunately, based upon the findings through various other steps undertaken, the examiner is of the opinion that fraud appears to exist, then a list of suspects indicating the kind of wrongdoings possibly committed, is compiled. Each of these suspects may need to be interviewed, individually or jointly. These interviews are those which are used for two purposes. One purpose is to provide a fair chance of explaining and an opportunity of being heard. The other purpose is to confront evidence to the suspects, or confront one suspect with another where their submissions/statements are contradictory. This stage is very challenging in the final evaluation because the suspects are likely to be antagonized and may offer considerable resistance. Interviewing skills are a science in themselves. One of the best ways to go about an interview at the exit stage or in interrogation or confrontation is to make a questionnaire docket in advance incorporating all possible questions to trap a fraudster to establish the innocence of any other suspect.

Evaluation of Facts

When the fraud examiner reaches a stage where he has exhausted all possible means of corroboration, substantiation, or collection of information, it is essential for him to review all facts and evidence in totality without losing focus on the objective. Issuing a report is likely to have serious ramifications and could

have a serious impact on the future and careers of a person or the organisation. Therefore considerable deliberation and micro-macro evaluation is vital. All clues must fit and all facts must be in harmony. Where findings suggest that a fraud appears to exist, a wonderful approach can be adapted from the 'Mimamsa doctrine'. It provides a structured, balanced and equitable method of conducting an inquiry and reaching a conclusion. i.e.,

1. Definition of the subject matter.
2. Enumerating doubts of the subject matter.
3. The third step is placing forward arguments *against* the doubts'.
4. The fourth step is to furnish rebuttals to the arguments in 3 above.
5. The fifth and final step is to come to the conclusion'.

An illustration of how process can go through in a case of an assignment inquiring into allegations of vendor bias against a purchase manager could be briefly explained as follows: After all the steps prior to the evaluation of evidence stage are carried out, the tenets of the Mimamsa doctrine could envisage the examiner overseeing the entire assignment as follows:

1. The purchase manager is guilty of favouring a vendor which is detrimental to the interests of his employer.
2. The examiner comprehensively lists out all doubts:
 - All allegations were anonymous.
 - The purchase manager was good in his work otherwise.
 - Several other vendors. were happy with him and had a good opinion also.
 - Past record of the purchase manager from earlier employments did not reveal any negative aspect.

3. There were several red flags:
 - Phenomenal growth of 150 % in business volumes.
 - The vendor's credentials were poorer and not comparable to some other vendors whose business volumes had dwindled in the relevant period.
 - Direct evidence available through audio recordings and video recordings of the purchase manager and the vendor at external places where such clandestine business deals for mutual favours were struck.
 - Submissions from other employees about the manager's policies for the favoured vendor also supported the allegations.
4. The purchase manager had been given a chance to view all evidence and to provide contrary evidence or a defence for rebuttal of the above. The arguments provided were as follows:
 - a. Growth in business was on account of the exceptional performance of the vendor.
 - b. Submissions from other employees were rebutted by submissions from certain employees who were close to him.
5. The purchase manager had no answer to the audio and video recordings. Further, he could not explain why he had disregarded other vendors, whose credentials were better than the favoured vendor's. There were 'n' numbers of the evidence which were against the purchase manager. Thus the purchase manager was deemed to be dealing with fraudulent intentions and had favoured the vendor specified.

Reporting

The report may then be presented in a manner which explains the conclusion reached pursuant to the objective. The report must be fine tuned to be comprehensible to the person addressed to and using it. Hence the report may be drafted and structured

Various Steps which can be Considered in a Situation of Fraud Detection

appropriately for each case. While each case may have a different set of requirements, usually the following elements are important:

1. Definition of the objective and terms of reference.
2. Conclusion: Where applicable, a list of suspects and wrongdoing would be specified.
3. Findings
4. Investigation Methodology
5. Constraints and limitations
6. Recommendations
7. Appendices (statements or illustrations or quantification's of findings).

Tools and Techniques Used

Thomas Edison has said "There is great value in disaster". Setbacks can be viewed as impediments or opportunities. If viewed as impediments, the results will be mediocre, but if viewed as opportunities, results will bring new inventions."

There are several tools which can be used in fraud detection. Some of the tools commonly used are:

1. **Computers and file interrogation (or Audit) software**
2. **Mathematical Tools and Statistical Tools**
3. **Electronic or digital tools**

Computers And Audit Software

There is a limitation to the amount of work that human effort can achieve. More often than not a voluminous job has to be carried out in a limited period. In a typical fraud investigation, one is faced with a situation, where the information is meagre, explanations vague, co-operation uncertain, transactions myriad and complex. All these are constraints which put the examiners in great difficulty where vast data, information and records are to be accessed, analysed, processed and evaluated as evidence, to facilitate reaching a conclusion. Computers in such circumstances offer remarkable assistance since they have the power of speed and precision. What is file interrogation (or Audit) software? There are two kinds of software that can be used for fraud detection.

- **Specific Audit Software:** There are products that are specifically designed and customised for auditors or investigators, which contain in-built tools that can be directly applied on many standard databases. The only limitation is the cost of such a product, which is very high but the results are focussed and effective.

- *Standard Application Software:* Alternatively, standard software spread sheets (Microsoft Excel, Lotus, etc.) or database management software (like Oracle, Access, SQL server, etc.) can also be conveniently used. However, this requires a high degree of familiarity with and awareness of their features and limitations and a small degree programming skill, and database knowledge, to adapt and apply the software to the specific needs of any given situation. The effectiveness, in application is directly proportional to the examiner's experience and resourcefulness.

What are the characteristics of computers and software tools which are useful in fraud detection?

- *Perform more in less time:* Computers can perform at an amazing that is measured as a millionth part of a second. Thus, data examination that can be completed in a given time outweighs work done by not one but several human beings collectively.
- *Perform substantive checks even on entire populations:* Data transactions being complex and large in volumes usually permit only a small sample to be examined and there is always a possibility of ignoring transactions infected with frauds. For example it would be inconceivable to examine 10000 paperless purchase transactions in a SAP R3 ERP system implemented for accounting and inventory modules. However, when an analysis is done on computers, checks and tests can be carried out on the entire data without the exception of any transactions which is humanly impossible.
- *Can query large databases through sophisticated analytical tools in seconds:* Similarly, it is humanly impractical, if not impossible, to locate duplicate bill numbers of any vendor in even say 500 transactions in a year. But computers could locate such duplicate records within a fraction of a second. There is worldwide research on various theories that facilitate identification of unnatural (fraudulent or error prone) data not conforming to the general pattern. Thus, intra-period, inter-division, inter-company or industry comparisons are possible by use of such theories or tools. Benford's Law

is one such revolutionary tool which was lying in the archives for years for want of a tool such as a computer to carry out digital analysis on large databases. This law has been explained in this chapter elsewhere.

- *Detection of risks and errors on account of users' untested programs:* Any software implemented by the users or auditees needs testing online constantly because today's world is dynamic and constantly changing. Unforeseen situations could permit an error or misuse. Therefore if an examiner is equipped with a tool at par with the software used by the user or the auditee, he can evaluate even more meaningfully. A file interrogation software is one such tool which can replicate a processing activity and the report can be compared with the actual report generated by the user software. If there are differences they need to be investigated and the impact ascertained. The reports generated by the user software on investigation queries could prove to be erroneous.
- *Reduction of dependence and reliance on one or a few technically qualified EDP technicians of the users or the auditees,* who could be encouraged to have fraudulent intentions. In most situations since the EDP is a highly technical area usually no one would question them because of ignorance of technical issues. This sometimes encourages fraudulent motivation because there is no fear of getting caught. Use of file interrogation software actually addresses this issue. Thus, such EDP managers are unlikely to mislead the examiner if such a file interrogation exercise is used and chances of deception on their part being caught are brighter.
- *Secrecy:* Secrecy is the key to the conduct of any fraud audit assignment. The examiner can conduct an exercise of gathering audit evidence through digital tools progresses in a covert way. By providing separate terminals for access and separate log-in's and passwords he can examine and collect data furtively and evidence can be used later to confront the perpetrators. Therefore, the fraud detection exercise, even the areas examined, the extent of checks applied, could be easily carried out in a veil of secrecy without the users

understanding, or being aware of the areas or the strategy of examination.

What are the typical fraud detection tasks for which software tools are used:

- *Locate Gaps in documentation.* Software tools are used to throw out missing sequential numbers, in millions of records. For example:
 - (a) Missing Cash Receipts which could denote cash suppression
 - (b) Missing Goods Receipt Notes, which could denote falsified material receipts or shortages in supplies permitted to favoured vendors.
 - (c) Missing Delivery Challans / Invoices which could suppress sales to customers.
- *Identify duplicates or replicates.* Converse to the above, software tools can be used to detect more than one entry of similar transactions for fraudulent purposes. Following are few examples:
 - Duplicated bills could mean excess or double credit to suppliers or to inflate expenses to siphon out funds.
 - Repetition of same employee code could indicate double salary payments.
 - Same cheque numbers from customers could be for suppressing recoveries.
- *Application of advanced mathematical and statistical tests.* Use of Benford's Law, Relative Size Factor Theory (RSF), and several other statistical tools is possible only on account of computers and software. Software tools if applied in conjunction with mathematical tools and statistical tools, can be used to detect coding errors, incredible frauds or deceptions and for plenty of other analytical purposes. One can get customised views due to which, decision making is rendered much easier. If data is presented in the light of a particular scenario being examined, decision making is focussed. Suppose one wishes to check the performance of a particular vendor, for say, timely deliveries and the number

of purchase returns in each month, the data has to be retrieved from a huge database of 100 such vendors. Though the data is there, it is not available in a form and manner to decide whether the performance is satisfactory. Audit software facilitates this by providing a window to view data filtered for that vendor, presented with delivery delay reports, purchase returns etc. The data can be neatly classified or stratified to get an overall view of the transactions. This bird's eye view is some times useful to set a direction to the specific areas and the extent of coverage.

Use of Mathematical and Statistical Tools for Detection of Errors

Some of the commonly used mathematical and statistical tools in fraud detection are:

- a) Benford's Law or the power of one
- b) Relative Size Factor
- c) Vedic Mathematics

a) Benford's Law

There is one astonishing tool which perhaps may revolutionise auditing, investigation and perhaps any data validation process in the current millenium. A professor in a college employed the following test to find out students who were untruthful. He asked his students to undertake a homework exercise of flipping a coin 200 times and noting down the results against each flip of the coin as "H" or "T". The next day when he was going through the homework results, within minutes, he could identify those students who had been deceitful and had 'faked' the results, i.e. those who had written the results without bothering to flip a coin 200 times. By using a mathematical tool of probability he knew that in an exercise of flipping a coin 200 times, a continuous run of Heads (H) or Tails (T) will appear at least six times in a row at some point in the 200 flips. Most 'fakers' or cheating students would not know this and their false reports did not include these continuous 'H' or 'T' six times even once. They were easily identified with the aid of this tool. That tool is the amazing first digit theorem or Benford's Law using digital analysis tools. It is also referred to as the power

of one. This astonishing mathematical theorem is a powerful and relatively simple tool for exposing errors, frauds, sloppy accountants, embezzlers, and even computer bugs. This has remained in the archives and been ignored for years, since 1938. What exactly does this law explain? In simple words any body of numbers contains numbers having digits 1 to 9 placed together differently for each observation. Intuitively, and also by the general law of probability, most people assume each digit could be *any* number from 1 through 9 i.e. probability of 1/9 or 11.1 %. All nine numbers would be regarded as equally probable in any place. However, as Dr. Benford discovered, this is not true. Each digit, in a number, in a body of data (natural number populations,) has an *expected* or defined frequency of appearance in the population. For simplicity, this guide deals with the appearance frequency of only the left most or the first digit in each number. Benford found that each of the nine digits **do not** have an equal probability of appearing. The chance that the first number in the string will be 1 **is 30%** as against common sense probability of 1/9 or 11.1 %. The probability of digit 2 appearing is expected about 17.6 percent. The following table indicates the expected frequencies as against 11.1 % or equal frequencies as what one would reasonably expect for all digits from 1-9 in the left most place in any number in a population:

First Digit Normal Expectation		Benford's Expectation %
1	1/9 or 11.1 %	30.10
2	1/9 or 11.1 %	17.60
3	1/9 or 11.1 %	12.50
4	1/9 or 11.1 %	9.70
5	1/9 or 11.1 %	7.90
6	1/9 or 11.1 %	6.70
7	1/9 or 11.1 %	5.80
8	1/9 or 11.1 %	5.10
9	1/9 or 11.1 %	4.60

This table was compiled after sheer hard work on widely disparate populations such as a day's stock quotations, a tournament's tennis scores, the numbers on the front page of The New York Times, the populations of towns, electricity bills in the Solomon Islands, the molecular weights of compounds, the half-lives of radioactive atoms and much more. How does this help investigators or auditors? The one word answer for this is 'phenomenally'. The application of this law in auditing can lead to amazing discoveries in terms of errors or frauds. Data validation and analysis of a new dimension is now possible. Most accountants or embezzlers would not know that any error or fraud is very likely to be caught or trapped by digital analysis using this amazing theorem. This is because a material error or a fraud, influences a natural number population and consequently the data set loses its digital properties as predicted by Benford and a digital analysis would easily throw up the anomalies for an auditor to concentrate upon. Thus this law facilitates an examiner to virtually focus his attention directly on fraud or error prone areas. It is believed that such digital analyses using this law are successful about 68 % of the time with the limited knowledge that humans possess as of date, as regards this law and its potential.

How does this law reveal frauds and errors? Simply stated, this law provides a barometer of percentages of expectation of digits in observations in a population which need to be compared with actual percentages for assurance. For example it says that from the total observations in a population of natural numbers, 30.1 % *must* begin with the number 1, 17.6% with the digit 2, 12.5% with the digit 3 and so on.. To illustrate, out of 500 cheque payments in a year, at least 150 (30%) must begin with '1' such as payments of Rs. 100, Rs.1200, Rs. 19, Rs.100000 and so on. If by digital analysis and computer aided tools the examiner finds that there are say 165 transactions beginning with 1, then there is a strong chance that there is an error or fraud in these transactions beginning with '1'. The actual population is stratified or segmented for transactions beginning with each digit and these transactions

are counted and summarised and their percentages to the total population are matched with Benford's (per table given earlier) expectation percentages as follows:

Transac- tions Beginning with:	No. of Transac- tions	% to Total Transac- tions	Benford's Expected %	Variance	Remark
1	165	33.00	30.10	2.90	Error/Fraud Expected
2	88	17.60	17.60	0.00	No variance
3	63	12.60	12.50	0.10	Nominal variance
4	49	9.80	9.70	0.10	Nominal variance
5	38	7.60	7.90	-0.30	Nominal variance
6	33	6.60	6.70	-0.10	Nominal variance
7	28	5.60	5.80	-0.20	Nominal variance
8	26	5.20	5.10	0.10	Nominal variance
9	10	2.00	4.60	-2.60	Error/Fraud Expected
Total	500	100			

The examiner would need to examine the heavy variances to determine whether frauds could exist. It would be relevant and important to mention here that the author of this technical guide was extremely sceptical of this law and did not really expect such digital frequencies to appear in any audit data, till he actually tested it. He tried out this test using audit software in an engineering company on a population data comprising cheque payments for the entire company running into a volume of about 30000 transactions for a quarter. This test was independently conducted by someone different from the audit team. The results

were amazing. The actual frequencies matched quite closely with the Benford's expected frequency distribution as given in the table above. Further, the actual audit results did not reveal any material discrepancy or fraud as per the independent audit team's audit findings which seemed to further prove the validity of Benford's Law. However, the above is a positive test and may not be convincing enough. What is really important is also to know whether this works where there *is* an error or fraud.

b) Relative Size Factor

Accounting manipulations stemming from intelligent planning can be easily camouflaged in vast data populations, and, even if noticed, can be explained away as errors. Such manipulations are, more often than not, revealed by accident. However, there are certain tools which can facilitate detection of such frauds and one of them is a mathematical tool called 'Relative Size Factor' (RSF).

The RSF is simple to understand: In a group of any given transactions, it is a ratio of the highest value divided by the second highest value. To elucidate, a vendor's statement of account had the following invoice values: Rs. 10,000, Rs. 12,000, Rs. 3,400, Rs. 7,600, Rs. 15,000. The RSF is the ratio of the highest value 15000 divided by the second highest 12000 i.e. $5/4$ or 1.25. If the RSF exceeds 10, then there is a very strong possibility that there is something wrong and further inquiry is necessitated. For example, if in the above case the vendor's highest bill was Rs. 1,20,000 (instead of Rs. 15,000) the ratio of 10:1 is obviously inconsistent. Of course, this RSF is meaningful only where volumes of transactions are high because, in essence, what the investigator is attempting to do is to find out what is out of the ordinary. The following example is one such case where the RSF revealed manipulation of a staggering value.

In an electronics company, there were several regional offices across the country that had huge inventories of finished stocks, tools and spares. Since inventories at each regional office were huge, the company management insisted upon monthly summarised region wise inventory reports. Its internal auditors also verified stocks on a quarterly basis. In one of the regional offices, there was a devastating fire, in which every item of stock,

documents and accounting records was gutted. An insurance claim was lodged, and the insurance company appointed surveyors to assess the claim. The claim was made on the basis of the previous month's inventory adjusted with the current month's sales, purchases, issues and dispatches reported to the head office as per records available there. The internal auditors had back-up data on a computer floppy of the last inventory valuation carried out about a month ago. Taking a copy of this data from the auditors with the consent of the management, the surveyor applied a series of tests on the inventory data, which had details of quantities and rates of about 5000 items. He then applied the RSF test on the rates of items of the inventory. Using digital techniques, he could filter out about 176 items, which had RSF 10:1 or more. He saw something unusual; all the 176 items had RSF of either 10: 1 or 100:1. On scrutinising them further, he found that all these items were relatively small value items. Where an item was, say, 50 paise, the decimal place had been shifted by two zeroes to make the rate Rs. 50. In certain cases the decimal place was shifted by one zero e.g. an item of Rs. 4 was made Rs. 40. The effect of both these was to inflate the rate and consequently the overall inventory value also. He verified the rates of these items by obtaining quotations from other vendors. The results confirmed that the values were grossly overstated. By applying realistic rates, the inventory value came down by Rs. 1.3 crores. A meeting with the top management was held to appraise them of the reduced value of the claim. A detailed investigation later showed that the regional office under a particular sales zonal manager, had huge shortages of certain finished stocks which had been clandestinely sold in cash. Such shortages had to be cleverly camouflaged in the management inventory reports. This was because, a fall in the inventory value would have been noticed and questioned and to be able to show a sufficiently large inventory value, the zonal manager had to contend with the internal auditors who were frequently physically verifying stocks as well. How was the manipulation done? Since physical quantities were short, and since auditors would certainly verify physical stocks of the high value items, therefore, the only other way left was to manipulate the rates. Accordingly, small priced C category items were selected where quantities were high, and the decimal places in their rates were moved rightward to inflate the inventory value and to offset the shortfall in stocks of finished goods. It was a

calculated risk that these rates would not be verified by the auditors because the items affected were the very small miscellaneous 'C' category items. Even if any of these fell into the sample verified and were queried, the manager would feign ignorance and rectify that particular item rate and pass it off as a data entry error. The fraud was of such a serious dimension that it was revealed that even the fire was not an accident. However the point of importance here is the manipulation of the rates which went unnoticed from a population of 5000 items. It might have been revealed as an error but not as a fraud but for the RSF.

This RSF is therefore an important tool now used by not only examiners, auditors but also management in order to highlight inconsistent data patterns to reveal manipulations

c) Vedic Mathematics

India has given the world '0'. The power of zero is phenomenal. There are 16 sutras or axioms in vedic mathematics, some of which provide 'visual' solutions or solutions using mental techniques. It is perhaps possible to make practical use of these sutras in certain situations.

Particularly where data or information validation can be done by using the appearance of zero or nil values in any data set. Situations, where data, information or records are destroyed or lost, by accident or fraud, provide a natural camouflage for all kinds of manipulations. Plenty of insurance claims are known to have been inflated by altering data. For example, in case of a 'loss of profits' claim, the claimant will try and inflate past sales and profit figures to maximise his deemed profit for the claim. Further, in most of these cases, the claimant always expresses his inability to provide sufficient evidence, on account of loss by fire even though the evidence actually may not be even partially destroyed. In these situations, mathematical axioms and tests of 'reasonableness' using human judgement are the only tools which are effective in ferreting out inaccuracies and even deceptions. Vedic mathematics is one such tool.

Electronic and Digital Tools

Lot of other new tools are being invented almost on a daily basis with greater and greater facilities and enhancements. Some of

those which an examiner or even an auditor can use effectively are:

- *Voice recorders*. These are like any other recording device such as a cassette recorder, but usually smaller in size so as to enable even covert or clandestine recording. There are small audio machines which are voice sensitive or sound activated so that only if there is a sound they are switched on automatically. Modern voice recorders are really so small and sensitive that they can be fitted easily upon the person without being noticeable. The innocent looking pen could well be a recorder.
- *Video recorders*. Handy cameras, video cameras of different shapes and sizes which can fit into small pouches and handbags and take surreptitious shots of an activity or conversation or meetings are common. These could be extremely useful in field audits and sting operations.
- Special magnification lenses or glasses for checking handwriting or erasures for alterations are also available. They are used to evaluate specimen signatures or distortions in documents. However these can be used only with experience or technical qualifications.

What is important is not the kind of electronic or digital tools but what they can do. The concerned experts will usually guide the examiner as to the kind of tools which may need to be hired. Where and how they have to be used and for what purpose is the key aspect. All these tools today are digitalised and readable and compatible with most computers. Their results can be easily downloaded and repeatedly reproduced multiple times without any adulteration in quality. Video films can be subjected to the same edit mode cut and paste operations as in word processing software, slow motion and special effects etc.

Thus tools play an important role in an investigation. However, the actual creativity, imagination and expertise of the examiner have to be applied to scale greater heights and achieve much more meaningful, penetrative and focussed results. Tools can be effectively used only if they are built into the fraud detection assignment with experience, foresight, judgement and vision to provide meaningful and penetrative findings.

Appendix D

Internal Factors that Reduce the Probability of Fraud, Theft and Embezzlement Include :

I. Prevention Measures

A. Internal accounting controls

1. Separation, . of duties
2. Rotation of duties
3. Periodic internal audits and surprise inspections
4. Development and documentation of policies, procedures, systems, programmes and programme modifications

B. Computer access control

1. Identification defences
2. Authentication defences
3. Establishment of authorisation by levels of security

II. Detection Measures

A. Logging of exceptions

1. Out of sequence, out of priority and aborted runs and entries
2. Transactions that are too high, too low, too many, too unusual (odd times, odd places, odd people)
3. Attempted access beyond authorisation level

4. Repeated improper attempts to gain access (wrong identification, wrong password)

B. *Variance reporting*

1. Monitoring operational performance levels for
 - a) Variations from plans and standards
 - b) Deviations from accepted or mandated policies, procedures and practices
 - c) Deviations from past quantitative relationships, for example, industry trends, past performance levels, normal profit and loss (PandL) and balance sheet ratios

C. *Intelligence gathering*

1. Monitoring employee attitudes, values, and job satisfaction levels
2. Soliciting feedback from customers, vendors and suppliers for evidence of employee dissatisfaction, inefficiency, inconsistency of policies, corruption or dishonesty

APPENDIX E

Internal Factors that Enhance the Probability of Fraud, Theft and Embezzlement Include:

I. Inadequate Rewards

- A. Pay, fringe benefits, recognition, job security, job responsibilities

II. Inadequate Management Controls

- A. Failure to articulate and communicate minimum standards of performance and personal conduct
- B. Ambiguity in job rules, duties, responsibilities and areas of accountability

III. Lack of Inadequate Reinforcement and Performance Feedback Mechanisms

- A. Failure to counsel and take administrative action when performance levels or personal behaviour falls below acceptable standards

IV. Inadequate Support

- A. Lack of adequate resources to meet mandated standards

V. Inadequate Operational Reviews

- A. Lack of timely or periodic audits, inspections, and follow-through to ensure compliance with company goals, priorities, policies, procedures and governmental regulations

VI. Lax Enforcement of Disciplinary Rules

- A. Ambiguous corporate social values and ethical norms

VII. Fostering Hostility

- A. Promoting or permitting destructive interpersonal or interdepartmental competitiveness

VIII. Other Motivational Issues

- A. Inadequate orientation and training for legal, ethical and security issues
- B. Inadequate company policies with respect to sanctions for legal, ethical and security breaches
- C. Failure to monitor and enforce policies on honesty, loyalty and fairness
- D. General job-related stress or anxiety

APPENDIX F

Use of Computers and Software in Audit and Fraud Detection

Advanced Use of Software in Audit and Investigation

Fraud detection has always been a creative process and the examiner's judgement, skills, and experience play an important role in the entire process. While the elementary documentary tests of data validation are essential, they are not always sufficient to achieve the desired objectives. Towards the end of any investigation, in order to achieve the objectives, he must also view the findings both on a macro and micro basis, and arrive at conclusions based on, control and substantive tests' results, data trends, and consistency of the data with the given facts in the control environment. However, it's the last point in which the use of file interrogation software phenomenally increases the depth and extent of the investigation; this is where the *advanced* application of the software comes in. Even in a standard audit situation, after all the routine control and substantive tests are satisfactorily applied and results evaluated, the auditor takes a macro look, in the context of the audit objectives, to satisfy him/herself that all the clues or facts fit properly. This is the place where the expertise supported by the software tool can perform miracles in terms of results and findings. What should be done at this stage, is to compile Data Query Models (DQM) to test the worth of all the earlier findings with the facts in the control environment. Quite simply, such DQMs are programs, or macros built using software for specific queries. These are possible even in simple spreadsheets, as well as in advanced audit software.

The strategy for preparing DQMs always stems from the examiner's study of the auditee's environment, the control strengths, and the regulatory statutes applicable. The information he/ she collects provides various clues in the form of facts and conditions that govern the various transactions, operations and the

activities under scrutiny. Based on these clues, the examiner can build up a DQM that can be applied to test the fulfillment of conditions or facts that affect the activity. He/she may require the aid of an IT manager to provide technical assistance, or achieve the desired reports. This can be more easily understood from the following example.

An auditor found that travelling expenses in a certain company were high (as well as voluminous), and controls were weak. Management had not insisted on air/train ticket receipts, and had been remiss in monitoring travel expenditures. In this context, the auditor wanted to ascertain whether there was a possibility of any inflated or false travel claims. He made a list of all the metro cities to which senior employees' travel was high. He also obtained from a travel agent the details of flight and train connections, and the days on which such flight/ train connections were available from the city in which the company was situated. He asked his IT manager to create a DQM which would filter the client's travel expenses, and each of these were further filtered by city, with details of days and dates of travel. The DQM was required also to compare the dates of actual travel with the dates of flight and train connection~ available, which were obtained from the travel agent, and generated exception reports. These exception reports were expected to spot instances where any person had travelled to any city where the air/train connection was unavailable. Sure enough, the report threw up four tours made by the same person to a city on days when the air/train connection was not av~~able. On making further inquiries, the auditor found that this person's expenditures were supported by fictitious bills for hotel, food and conveyance during his four trips. Such a comprehensive test was obviously impossible manually wherein, at best, a sample test would have been applied. However the DQM, compiled through audit software, made it possible to check the travel of every employee for the entire period under audit, with accurate results.

Introduction on Concurrent Audit

Concurrent audit is a systematic and timely examination of financial transaction on a regular basis to ensure accuracy, authenticity, compliance with procedures and guidelines. The emphasis under concurrent audit is not on test checking but on substantial checking of transactions

The concept of concurrent audit has been introduced to reduce the time gap between occurrence of transaction and its overview or checking. The concurrent audit serves the purpose of effective control as it is normally conducted by organisation.

Objectives of Concurrent Audit

Concurrent at a bank branch provides a supplementary management tool for an on the spot examination of transactions /activities at the branch on daily basis. This audit at a bank branch involves a systematic examination of all the transactions on a continuous basis to ensure accuracy, authenticity and due compliance with internal systems, procedures and guidelines of the bank.

The objectives of concurrent audit are:

- a) To supplement efforts of the bank in carrying out simultaneous internal checks of transactions and compliance with the systems and procedures of the Bank.
- b) To perform substantive checking in key areas and on-the-spot rectification of deficiencies to preclude the incidence of serious errors and fraudulent manipulation.
- c) To reduce the interval between a transaction and its examination by an independent person not involved in its documentation.
- d) To improve the functioning of the branch, leading to upgradation and prevention of fraud.
- e) Compliance with internal control as well as RBVGOI guidelines.
- f) Identification of areas/ activities requiring corrective action and urgency.

Chapter-VII.13

Role of Concurrent Auditor

The main role of the Concurrent Auditor is to supplement the efforts of the branch in carrying out simultaneous internal check of transactions and other verifications and compliance with the stipulated procedures laid down. In particular, it should be seen that the transactions are properly recorded / documented and vouched.

The most important feature of the Concurrent Audit System is the spot rectification of irregularities and the implementation of systems and procedures of the Bank.

A Concurrent Auditor may not sit on judgment/decisions taken by a Branch Manager or an authorized official. Concurrent Auditors are not meant to interfere or block the daily working of the respective branches / offices. The purpose of their presence is to provide for "a second cool look" on the operations. The presence of the Concurrent Auditor should convey the message to the staff working at the branch in that the activities of the bank branch are being continuously supervised.

The Concurrent Auditor will Assess whether transactions performed or decisions are within the policy parameters stipulated by the Head Officer they do not violate the instructions or policy prescriptions of the RBI and that they are within the delegated authority and in compliance with the terms and conditions for exercise of the delegated authority.

In very large branches-which have separate sections dealing with specific activities, Concurrent Audit is a means to the in-charge of the branch to ensure that the different sections function within parameters and procedures on an on-going basis.

Coverage

The Reserve Bank of India has issued certain guidelines for the conduct of this audit. These guidelines are mandatory and all

banks are required to cover 50 percent of the total deposits and 50 percent of total advance under this audit.

The coverage of concurrent audit includes:

- A. Department/Divisions at the Head Office dealing with treasury functions viz. investment, funds management, including inter-bank borrowings, bill rediscount and foreign exchange business service branches are to be subjected to concurrent audit.
- B. The coverage of branches should ensure that concurrent audit covers:
 - a) Branches whose total credit and other risk exposures aggregate to not less than 50% of the total credit and other risk exposures of the bank, and
 - b) Branches whose aggregate deposits cover not less than 50% of the aggregate deposits of the Bank. These branches would include;
 - ✓ Exceptionally large branches.
 - ✓ Very large and large branches
 - ✓ Special branches handling forex business, merchant banking business, large corporate/wholesale banking business and forex dealing rooms.
 - ✓ Branches rated as poor/very poor
 - ✓ Any other branch where in the opinion of the bank concurrent audit is desirable.
- C. Branches subjected to concurrent audit should not be included for revenue/ income audit.

Areas Covered

The concurrent auditor has to examine all the transactions of the branch simultaneously or at best on the next day. The concurrent audit should cover areas like cash, deposits, advances, foreign exchange transactions, bills, remittances, sundry and suspense accounts, clearing transactions, ancillary service, govt. business, house-keeping, customer service/complaints, submission of returns, computerized operations, profitability and revenue leakage. The areas mentioned are only indicative and the concurrent audit should cover the entire operations of the branch. The details of these areas are given in Annexure I to VII.

Audit Procedures

The auditor, in performance of his duties, should ensure that all the areas of branch operation have been covered. The audit should be performed as per the checklist given in Annexure I to VII later in this material.

Audit Papers

The auditor should record the audit plan as per the checklist and the format of audit report given by the respective banks. It includes the circulars, terms of engagement, scope of work etc given in the engagement letter.

The Concurrent Auditor should keep all the working papers on record which are used in finalizing the reports. The following papers can be kept in permanent audit file:

- ✓ Letter of engagement, undertaking/comment by the firm to the bank Audit checklist.
- ✓ Information regarding branch business, data, nodal officer, status of branch, whether computerized/parallel category of branch, etc.
- ✓ Performance of monthly, quarterly, annual report revenue report.
- ✓ Correspondence with the bank for any matter.

Current file includes - all other papers relevant to the audit, mainly:

- ✓ Branch Audit Programme.
- ✓ Branch's statement as on the data of the report on which basis it is prepared.
- ✓ Periodic correspondence with the concerned departmental officer.
- ✓ Irregularities intimated to the branch manager.
- ✓ Discussion of the audit report.
- ✓ Particulars of big borrowers, depositors etc.
- ✓ Circulars received from RO.

Besides, in order to keep correspondence between the incumbent and concurrent auditor it is in interest of the auditor to record his observation in a register and bring them to the notice of concerned official on daily basis. In some banks this register is mandatory and to be kept in the branch manager's custody.

Reporting Systems

The idea behind the concurrent audit is to effect on the spot rectification of irregularities in the operations of branch. The Concurrent Auditor should examine the transactions/ decisions at the branch the very next day. The audit shall be a daily affair i.e. the deficiencies or lapses in the normal working get rectified on spot. The irregularities found during the day should be intimated to the concerned officer for rectification. If not rectified immediately, it should be brought to the notice of the concerned department in charge for necessary action. Even if it can not be rectified, then the deficiencies or lapses in the normal working shall be intimated to the Branch Manager. The outstanding irregularities should be discussed with Branch Manager and his viewpoint taken into account while reporting.

The concurrent audit report should help the bank in monitoring the performance of the branch on a continuous basis in accordance with prescribed rules and regulations of the bank. The report format may be monthly, quarterly, half yearly and annually as per the terms of engagement of bank.

Special Report-Reporting on Frauds

The special report should be submitted by the Concurrent Auditor whenever he comes across any serious irregularity/frauds etc. It is expected of the Concurrent Auditors to get in touch with the higher authorities through the quickest means of communication depending on the gravity of the irregularity/fraud detected during the concurrent audit, besides sending a written special report to the higher authorities, explaining in clear terms the finding of the case stating why such a fraud took place. This aspect is mentioned in the scope of work/appointment letter given by the concerned bank based on the Mitra Committee recommendations. The purpose behind this report is to safeguard the interest of the bank.

Time Schedule for Reports

It is as per the terms of engagement or appointment of the Concurrent Auditor. Usually, monthly reports are to be submitted within seven days from the end of the reporting month and within ten days from the end of the reporting quarter, in case of quarterly reports.

Revenue Audit

The concurrent audit system is implemented to plug the loopholes in the system to prevent any revenue leakage. The Concurrent Auditor should conduct revenue audit checking on a daily basis and bring lapses to the notice of the branch head to rectify the same lapses to the notice of branch head to rectify the same. In areas where the branch disagrees with the auditors on account of interpretations and where the auditor still feels otherwise, such matters must be brought to the notice of the next higher level authority. In the audit report, besides undercharges detected and recovered during the period, the concurrent audit shall also

comment on the recovery of un-recovered undercharges reported in the previous report.

Revenue audit must be done on daily basis during the tenure of concurrent audit of branch. All items should be seen for report and recovery of short collection or excess payments. Unauthorized charges should be reported with remarks.

With respect to charges and overheads, it is essential to verify whether expenses incurred beyond branch powers were sanctioned/reported/confirmed by the sanctioning authority. Branches under concurrent audit will not be subject to revenue audit.

Relative Importance to Different Areas

The purpose of concurrent audit is substantive checking in key areas rather than test checking. The Concurrent Auditor shall daily go through all the vouchers and other books of the branch for the previous day and identify areas to be scrutinized in detail. In case the volume of transaction and deposit/advances at the branch are heavy and it is not possible for the person posted to conduct cent percent checking the next day, the concurrent auditors may first concentrate on high value transactions having financial implications for the bank rather than those involving lesser amount, although number wise these may be large. In any

case, the examination of all transactions as per prescribed norms should be done invariably. Generally, the following guidelines should be followed:

In certain areas such as off balance sheet items (LC's and LG' s), investment portfolio, foreign exchange transactions, fraud prone/sensitive areas, advances having outstanding balances of more than Rs.50 lakhs and accounts with less than Rs.50 lakhs if any unusual feature is observed, the concurrent auditors may conduct cent percent checking.

In the case of areas such as income and expenditure items, inter-bank and inter-branch accounting, interest paid and interest received, clearing transactions and deposit accounts, the checking

can be restricted to 25 percent of the number of transactions covering all higher value transactions and some of the other transactions. All interest paid over Rs.1 000/- must be checked.

Where any branch has poor performance in certain areas or require close monitoring in housekeeping, advances or investments, the Concurrent Auditor may carry out intensive checking of such areas.

The Concurrent Auditors should critically examine the working of each department of the branch themselves and identify problem areas and loopholes/ lacunae in the conduct of bank business at the branch level and offer suggestions to overcome them. The Concurrent Auditor should ensure enforcement / restoring of prescribed systems and procedures in the branch.

If any adverse remark is required to be given, the Concurrent Auditors should give reasons thereof.

The Concurrent Auditor should indicate the extent of checking in various areas in his report. If the same is given in the format in which the report is to be submitted, reference of this fact may be made in covering letter of the report.

Frequency of Checking Different Items

1. The guidelines given by bank in the scope of work, circulars issued from time to time are to be taken into account while conducting the concurrent audit.
2. The Concurrent Auditor shall have to devise their own strategies/time frame covering all the areas. The auditor should identify the areas at the branch which need greater attention, the areas which are to be regularly monitored, the items which are to be checked daily, and the items which can be checked less frequently.

The Concurrent Auditors should go through the previous reports such as statutory audit report, internal inspection reports, RBI inspection reports, and concurrent audit reports of the branch as well for this purpose.

A suggestive / illustrative (not exhaustive) checklist of items to be checked daily / weekly / fortnightly / monthly / quarterly / half yearly etc. are given in Annexure I-VII. If security checking has also to be more substantive and may be spread throughout the year.

The surprise element of cash/security items verification must be retained. While performing the concurrent audit.

Monitoring

While the basic responsibility of the incumbent in-charge to monitor all key areas will remain, the concurrent auditor shall have to monitor all the areas in housekeeping, credit management etc., on an ongoing basis with the purpose of bringing an improvement in the functioning of the branch.

The Concurrent Auditor should maintain a register and note down the position of branch/areas in this register e.g. arrears in Balancing of Banks, sanctions overdue for renewal, Adhoc limits, inventories not being checked/received on monthly basis/ limitation expiring during next 3 months, repayment of installments overdue by more than one month etc. The auditor should monitor progress in these areas with branch manager at least once a week.

Besides the aforesaid areas required to be followed up, the Concurrent Auditors may also note down the crucial areas of the branch, e.g., large advances - their vital terms, operations in accounts opened during last six months to ascertain the validity and authenticity of transactions in these accounts, date when different items were last checked etc. which will assist him in his daily working.

Removal of Irregularities

The Concurrent Auditor should make maximum efforts for removal/rectification of irregularities on the spot. Outstanding deficiencies/irregularities should be discussed with branch officials and their viewpoints should be reflected. The Concurrent Auditor should maintain a register where irregularities observed would be

Training Material on Internal Audit

noted down on daily basis. These irregularities need to be discussed with the branch manager his designate at the end of the day. Only pending irregularities not rectified should find place in the final report. Materiality of these pending irregularities should be spelt out clearly in the final report. The branch manager's view on these final queries should also to be noted down.

The irregularities pointed out in the previous monthly/quarterly concurrent audit reports may be dropped by Concurrent Auditor himself if the same has been rectified.

The Concurrent Auditor should get the guidelines implemented in respect of following sensitive areas on priority basis to avoid the occurrence of these irregularities:

- a) Morning checking i.e. checking of all computers generated supplementary, checksum generation checking, previous day's G.L, Day Book, Exceptional Transaction Report, Day beginning by System Administrator as per Computer Manual etc.
- b) Teller's reconciliation.
- c) Custody, checking and use of scrutiny forms.
- d) Balancing and checking of books.
- e) Safekeeping of AOF's, ledgers, teller cards etc.
- f) Use of password - by - the password holder himself and initialing each entry in Audit Trail/ Transactions list by, the password holder, and the same appears in the printout.
- g) Post sanction and periodic verification of securities.
- h) Correct provisioning of interest on deposits and advances and proper maintenance of the Interest Register.

Certain irregularities like excess cash, suspense entries, defects in AOF's supplementary ledger checking, bills, insurance etc., find place in many of the reports. Cash Ratio limit in terms of percentage and/or amount is fixed by the higher authorities and this should be complied with. Any variation is to be reported by the Concurrent Auditor. The Concurrent Auditor may permit a reasonable time for the completion of formalities.

In case the Branch officials do not cooperate in rectification of the irregularities, the Concurrent Auditor may contact/write to the higher authorities.

Compliance of prescribed systems and procedures in the branch is the primary responsibility of the staff and incumbent in charge. However, the Concurrent Auditors must take all necessary steps to ensure that there are no violations in the branch any more.

Infrastructure for Concurrent Auditor

Infrastructure facilities such as proper sitting arrangement, all circulars from controlling office, operating instruction/directive will be made available to the Concurrent Auditor.

Co-ordinator For Concurrent Audit

Concurrent audit is different from the normal statutory and other audit of banks, as this audit is a daily affair. Sometimes, there is resistance from staff of branches when such an audit is introduced.

It is recommended that there should be one person to work as the coordinator from the branch's side for the smooth conduct of the concurrent audit and rectification of irregularities. He will bridge the gap (if any) between the auditor and staff working at branch.

Extension Counters

If any extension counter (s) is/are functioning under the branch, checking of such extension counters should also be done at least once in a week, in case daily checking is not possible. In case of Service Branch check whether a fortnightly statement of branch accounts are sent to all local branches, and outstanding entries as per the statement are scrutinized. If the originating entries pertain to the service branch, duplicate advices are sent to the branches in other case it is called of the service branch is kept informed by sending advices from branches whenever we rectification entries are passed by branches among themselves without routing the transaction through service branch.

Annexure-G

Checklist-Daily

I. Cash

1. Verify daily cash transactions with particular reference to any abnormal receipts and payments.
2. Proper accounting of inward and outward cash remittances with the prescribed security measures adhered to and notings made in Cash Movement Register.
3. Verification of Cash Movement Register.
4. Whether the Branch is habitually holding cash balance beyond the cash retention limit or is there a need for it at the branch? Is it fixed rationally?
5. Whether exchange of cash between cashier is made after making entry in the register.
6. Verification of cash scroll and the token book with cashier's summary and Cash Abstract.
7. Expenses incurred by cash payment involving a sizeable amount (vouchers of high value of Rs. 50,000/- and above).
8. Verify whether Cash Remittance in Transit Account is reversed on the same day by debit to a proper head of account designated for it after receipt of proper acknowledgement/receipt where cash is remitted to a branch / bank.
9. Proper accounting of currency chest transactions, its prompt reporting to RBI.

II. Clearing

1. Proper accounting of inward and outward clearing on daily basis without keeping a bunch for future accounting.
2. Verify whether counter returns, inward and outward, are properly accounted for. In respect of cheques returned by other banks whether respective customer's account are debited.
3. Whether clearing difference arose genuinely and is duly adjusted?
4. Whether safeguards are observed to ensure proper handling and custody including returned instruments?
5. If the branch is independently handling clearing, whether the clearing account is brought to nil every day, if not, comments to be noted down.
6. Whether service charges / incidental charges as prescribed are charged for the cheques returned in clearing.
7. Whether drawings are allowed against uncleared cheques. Whether such cheques are referred through prescribed register and passed by the Branch Manager. If the drawings exceed the prescribed limit whether these are reported to the Controlling Authority. Examine whether interest was charged and report such omission in the Revenue Report.

III. Deposits

1. Verify whether proper introduction has been obtained on new accounts opened and credentials of introducer(s) verified.
2. Verify whether all relevant documents are obtained at the time of opening of accounts viz. Partnership Deed, Articles and Memorandum of Association, Trust Deed and Bye-laws etc.

3. Verify whether photographs of account holders are obtained, attested and pasted/fastened to the Account Opening Form.
4. Verify whether the payment of Term Deposit beyond Rs. 20,000/- is done through the credit of Current/Savings Bank A/c. or by Manager's cheque.
5. Verify all interest payments above Rs. 2000/- of the previous day with regard to its accuracy.
6. Verify whether service charges for the return of cheques, issue of cheque books, carrying out standing instructions and minimum balance charges are levied as per prescribed norm.

IV. Remittances / Bills for Collection - Inward and Outward

1. Verify whether proper accounting of inward and outward remittance transactions is done.
2. Verify whether DDS/TTs/MTs of Rs. 50,000/- and above are issued through accounts and not against cash.
3. Verify whether DDS/TTs/MTs of Rs. 50,000/- and above are issued through accounts and not in cash.
4. Verify whether prescribed service charges by way of exchange, commission, out of pocket expenses, interest, overdue interest in respect of all remittances, bills purchased and collection items are recovered.
5. Verify whether IBCNs (Inter Branch Credit Note) are prepared and sent promptly.
6. Verify physically the inward bills on hand and post parcels tally with records.
7. Verify whether returned bills are debited to "Past Due and Dishonoured Bills" and followed up as per guidelines.
8. Verify whether documents of title viz, Transport

Receipts, Railway Receipts are obtained in favour of the Bank and whether transporters are on the IBA approved list.

V. Advances

1. Verify that disbursements are allowed against proper sanction, within sanctioned limits and drawing power.
2. Verify that in case of advances disbursed beyond the discretionary powers of the Branch Manager, prior permission has been obtained from the competent authority. In case competent authority could not be contacted and emergency powers have been exercised/drawings in excess of sanctioned limits have been allowed in exigency, verify whether weekly returns are being submitted without exception to the controlling authority and/or ratification sought subsequently.
3. Verify whether the permanent incumbent confirms the decisions of the officiating Manager.
4. Verify whether EMI in loan accounts has been correctly calculated.
5. Verify interest received vouchers in respect of loan/advance accounts closed on the previous day.
6. Verify whether bills are purchased as per terms of sanction and proper margin is maintained as per sanction.
7. Verify whether pre-sanction verification is done before sanction of BP limits.
8. Verify whether clean bills/cheques purchased are not in the nature of accommodation bills or kite flying operations.

VI. Foreign Exchange

1. Verify that L/C and Bank Guarantee are issued as per terms of sanction and charges are recovered as per FEDAI Rules / HO Guidelines.

2. Verify that packing credit released is backed by L/C or confirmed order, ECGC cover is available and the ECGC terms are complied with. In case of running packing credit accounts, whether RBI guidelines are complied with.
3. Discounting of Bills under L/C - whether prescribed procedure like verification of signatures of the Issuing Bank has been followed and scrutiny report raised.

VII. House Keeping

1. Verify whether the branch head authorizes all debits in the Suspense Account.
2. Verify whether tear off sheets for HO Balances and IBR are prepared correctly and sent promptly.
3. List the Book/Register/Ledger/General Ledger Account heads not checked and/or not balanced. Latest balances taken, amount of balances short/excess, balances differences freeze out, if any, with remarks and actions taken.
4. Verify and comment on day-to-day writing, posting and checking of:
 - ◆ Supplementaries
 - ◆ Day Book
 - ◆ General Ledger
 - ◆ Progressive Register/Transaction sheet
 - ◆ Exceptional Transaction report
 - ◆ Check sum generated by computers
5. Scrutiny of daily vouchers with more emphasis on high value transaction. There should not be any debit to the Sundry Credit and if any debit has to be made voucher of these to be signed by incumbent in charge of branch only.

Annexure-H

Checklist-Weekly

I. Cash

1. Verify whether keys to Strong Room, Cash Safe, and Almirah for Security Printing Books are in joint custody of authorized officials?
2. Verify whether there is any entry outstanding in Cash Remittance in Transit Account for more than 3 days.
3. Verify whether the branch remits all its excess cash to link branch or Currency Chest.
4. Verify whether the branch remits its surplus balance with other banks regularly to the designated RBI centre.

II. Clearing

1. Whether credit for realized cheques are received promptly.
2. Verify entries which remain outstanding for more 2 days and check for action taken for their disposal.
3. Verify whether account with Main Branch is reconciled every week.

III. Deposits

1. Verify that letters of thanks are being sent to the new depositors as well as to the introducers in case they cannot come to the branch.
2. Verify that stop payment instructions are being recorded properly.

3. Verify that lien on Term Deposits is properly noted whenever Receipts are held duly discharged by the Depositors.
4. Whether the prescribed safety measures and guidelines for issue of cheque books/loose leaves are observed.
5. Verify whether the branch is following the guidelines issued by RBI and other statutory authorities with regard to all account opening forms obtained during the period including abstention of declaration of staff accounts should be verified.
6. Scrutiny of staff accounts to detect any abnormal transaction.

IV. House Keeping

Verify whether accounts with local branches of the Bank, SBI, and other Banks are reconciled.

V. TTS Issued and Paid

1. Whether there is non-dispatch/non receipt of confirmation.
2. Is there follow up for receipt of confirmation?
3. Is there any remittance in transit outstanding beyond 30 days? Whether relevant returns are sent.
4. Whether telegram/telex are sent on same day.
5. Whether branch claimed interest from other banks where there was delay and followed up the claim for receipt.

ANNEXURE - I

Checklist -Monthly

I. Cash

1. Surprise physical verification of cash in hand, foreign currencies, and foreign travellers' cheques on any day during the month.
2. Verify whether currency notes are sorted, stitched and bundled properly. As per latest RBI guidelines notes bundle is not to be stitched now.
3. Verify whether cut/mutilated notes are kept separately as per the RBI norms and disposed off.
4. Verify how many times the branch exceeded the Cash Retention Limit and action taken by the branch to dispose of surplus cash.
5. Verify if there is a large accumulation of soiled notes and steps taken by the branch for the disposal of soiled notes.
6. Verify that the receipt and delivery of Security Printing Books are properly recorded under joint signatures.
7. Physical verification of the Security Printing Books and tallying with the balance.
8. Check list on Cash Management.

The following checklist is illustrative in nature. This is a compilation of suggestions received from members associated with concurrent audit across the country.

1st Month	2 nd Month	3 rd Month
i.	Date of verification of Cash	
ii.	Amount of cash held as on the date of verification	
iii.	Cash retention limit of the branch	
iv.	No. of days when cash retention limit exceeded during the month/quarter and by which amount	
v.	What is the percentage of cut notes/coil out of total cash held as on date of surprise verification of cash	
vi.	Actual amount of cut notes held	
vii.	Whether cut notes are kept separately	
viii.	Whether "Cash discrepancy register" maintained and Excess/Shortages reported to higher authorities promptly.	
ix.	Whether surprise verification of cash done by officer other than joint custodian officer/manager	
x.	Whether cash movement register is maintained as per guidelines	
xi.	Whether the branch is maintaining records/registers relating to inward/outward cash remittances to currency chest properly and proper insurance cover has been obtained.	
xii.	Whether currency chest transactions are properly accounted and reported to RBI? (wherever applicable)	

II. Accounts with Other Banks

1. Verify whether large idle balances are maintained with banks and if so, the amount and for what period at a stretch. Ensure that the branch obtains full particulars of debits/credits in the account and entries are promptly recorded.
2. Verify any outstanding entry of a suspicious nature.
3. Verify whether TT Discounting Limit of the branch with SBI is adequate and the facility is properly utilized.

III. Deposits

1. Verify, if large cash deposits/withdrawals in all operative accounts are genuine and if in line with the volume and type of business of the account holder.
2. Comment upon the action taken in respect of frequent cheque returns and whether they are entered in the Register.
3. Verify whether the deduction of tax at source (TDS) from interest income on Term Deposits is done as per laid down procedure.
4. Verify whether Form No. 60 where the depositor does not have PAN is held on record and the same are submitted as per laid procedure.
5. Debits in the inoperative accounts:
 - (a) Verify whether inoperative ledgers are kept separately under the custody of the Manager/ Officer. Is it inoperative accounts ledger repetitive, can be combined if combined them the subsection names (a,b,c,d,e,f) will be change.
 - (b) Verify if inoperative accounts ledger and Specimen Signatures are kept under the custody of Manager/ Asst. Manager and access thereto is controlled.
 - (c) All transactions of Rs. 5,000 and above to be verified in detail/ reported and other entries be checked at random.
 - (d) Is there a close follow up of subsequent entries? Are they checked and found in order?
 - (e) Whether dormant/inoperative accounts are transferred to inoperative ledger. If not, it should be noted in the register and they should be transferred.
 - (f) Verify that all transactions relating to inoperative ledgers are allowed under the written authorisation of the Manager.

IV. Remittances/Bills For Collection - Inward and Outward

1. Verify whether registers prescribed by bank for these are up to date and the tear-off sheets/statements are sent regularly.
2. Verify whether branch detains Inward Bills/cheques/ collection items beyond the stipulated period.
3. Verify whether overdue bills are properly followed up/non-payment notices are served?

V. ADVANCES

It can be checked under following heads:

- (a) Documentation
- (b) Renewal of documents and time barred accounts
- (c) Bills purchased/discounted/import LC documents
- (d) Cash credit including temporary overdrafts
- (e) Loans and advances
- (f) Advances under consortium arrangement
- (g) Merchant Banking Business
- (h) Credit Cards

Documentation

1. Whether documents register is maintained up-to-date. Entries are made in this register and found in order. If there is any omission it should be reported.
2. Are all documents correctly executed in the latest revised prints of prescribed formats and properly stamped wherever necessary in terms of Stamp Act as per manual on documentation and as per circulars on the subject?

Training Material on Internal Audit

3. Where immovable properties are held as security by way of deposit of title deeds, verify title deeds register to see whether narration is written for additional limits and all formalities complied with.
4. Whether legal opinion and valuation by an engineer are obtained for all the mortgaged properties and the latest Encumbrance Certificate as well as tax receipts are obtained up-to-date.
5. Verify the correctness of documents.
6. All the documents should be examined and action initiated for rectification should also be scrutinized.
7. Ascertain authenticity of signatures of executants/ borrowers from respective borrower's current correspondence file.
8. In case of Limited Company:
 - a) Whether copy of resolution passed by Company's Board is on record for availing the credit facilities from the bank.
 - b) Whether the authorised signatories as mentioned in the board resolution have executed the documents.
 - c) Whether common seal affixed on the relevant document.
 - d) Whether bank's charge or modification thereof has been registered with the Registrar of Companies (by filing Form 8). Whether search of earlier charge is made.
9. Check classification of advances as per RBI's Prudential Norms.

Renewal of Documents and Time Barred Accounts

1. Verify limits/accounts falling due for review, renewal and action by the branch. Verify whether due date diary of review/renewal is maintained and required follow up done on those dates.

2. Whether the debts/decrees are time barred. Action taken to be commented.

Bills Purchased / Discounted / LCBR (Import LC Documents)

1. In case of Bills that have been returned without recovery, give details indicating date of return, reason for non-payment, status of goods covered, insurance protection, etc.
2. In respect of LCBR-whether goods are appropriately protected with Insurance.
3. Examine the total number of Bills and amount returned and recovered during the period under review.
4. Whether satisfactory credit report on drawees in respect of Bills/Drawers in respect of cheques are held?
5. Whether LC documents (LCBR) were verified with LC terms? Whether LC bill was rejected by the importer for any reason of non-compliance with LC terms, etc.
6. Whether cheque/bills are dispatched promptly, at least on the next day?
7. Whether interest/commission, as prescribed, are collected?
8. If any excess was allowed and not reported, mention the date of excess, amount name of the party, nature of facility, sanctioning authority, etc.,
9. Does the branch ensure dispatch of returned cheques by registered post if they are not collected immediately? In case any deviation is noticed, please give full details.
10. For supply bills, verify whether the branch ascertained the genuineness of the underlying contract and Power of Attorney registered in the Bank's favour?
11. What is the system of follow up for the recovery of returned bills? How long have they been kept pending?

Training Material on Internal Audit

12. Are sales against firm orders. Whether the bills relate to genuine trade transactions?
13. Are the goods covered generally traded items / dealt with?
14. Any unusual features noticed in the handling of portfolio of bills?
15. In respect of all overdue and returned bills, please examine and comment on the fate of goods and report details of such bills including LCBRs remaining unpaid after arrival of goods, indicating action taken by the branch.
16. In respect of export bills purchased and discounted, expressed in foreign currency, whether overdue bills were promptly converted into rupees under report to the central office.
17. Whether packing credit was adjusted where applicable.
18. Comment on cases where payment is received under reserve.
19. ECGC policy as applicable is held - Drawee Limit is mentioned for compliance.
20. Wherever LR is accompanied check whether they were issued by approved lorry companies?
21. Whether appropriate margin/exchange/postage has been collected as per sanction stipulation?
22. Whether the turnover in Bills limit reflects the true position of sales as evidenced from balance sheet? Large variation should be commented.
23. In case of Foreign Bills Purchased/Discounted for export on FOB and CandF terms, whether the contingency risks policy as per Head Office instructions and Exchange Control requirements.

Cash Credit Including Temporary Overdrafts

1. Whether the branch has identified and classified the advance in accordance with the guidelines of the RBI and the Head Office.
2. Report individually on accounts in which there are irregularities due to:
 - a. Excess drawing over drawing power.
 - b. Excess drawing over limit.
 - c. Deficiency in documentation.
 - d. Operations unsatisfactory/no operation.
 - e. Drawings against uncleared effects.
 - f. Non-inspection of securities.
 - g. Non-recovery/absorption of interest.
 - h. Not covered by sanction.
 - i. Unreported excesses.
 - j. Drawings not reflected by QIS where applicable.
 - k. Account not brought to credit as per sanction terms.
3. Verify whether passing of cheque is duly authorised through Cheques referred Register, where there are irregularities as mentioned above.
4. Whether excess over the limit/drawing power is covered by adequate security and prescribed margin is maintained?
5. Whether stock statements received contain Sundry Creditor's outstanding to calculate drawing power against paid for stocks.

Training Material on Internal Audit

6. Whether any spurt in inventory is noticed and verified for the source of funds.
7. Whether norms for inventory and receivable, wherever applicable is monitored.
8. Whether appropriate action is taken where the non-submission of stock statement persists for two months.
9. QIS I, II and III are studied critically and date are entered in a register for follow-up at the time of annual review-whether variations from projections are questioned and Considered realistic based on past performance and environmental outlook.
10. Adequacy/enforceability of insurance or insurable assets with appropriate risks, location, etc., is seen. Whether bank clause is incorporate.
11. Indicate cases where a delay in the recovery of interest is noticed.
12. Adhoc facilities allowed to continue beyond the stipulated period mentioned in sanction, to be highlighted.
13. Excess beyond the adhoc limit without report/confirmation and allowed to continue without recovery to be pointed out.
14. Concurrent Auditor should conduct inspection of units/godown/fixed assets/stocks under pledge and hypothecation in such a way that all the accounts are inspected at least once in every six months. Stock inspection report should be in the prescribed format as per the specimen attached. Examine whether stocks register is maintained.
15. During stock inspection, correctness of valuation and adequacy of stocks to cover the advance and obsolete/unsaleable aspects of stocks to be examined and reported.

16. In case where delay in the receipt of stock statement is persisting and where stock statements are not received, Concurrent Auditor should take up inspection such units on priority basis and assess the value of security available and report.
17. In respect of consortium advances, the Concurrent Auditor should conduct inspection as per decision of the consortium where the turn comes to the particular branch for inspection.
18. In cases of temporary over draft, comment when the account was last brought to credit and whether the relevant cheques were passed through the Cheques Referred Register and approved by the manager? Report excesses over the limit and those remaining overdue with details and whether the facts were reported to the controlling authority.
19. In respect of sick and viable units, report on the implementation of a nursing package, if any, progress in preparing a rehabilitation plan, whether the progress report are received and studied, and comment on the current health of the unit. Whether the matter was considered by BIFR, if so, status of references to BIFR. List out weak areas in the unit to be strengthened. Whether functioning of the unit is in accord with earlier projections submitted to the bank and approved.

Loans and Advances

1. Verify by surprise goods pledged to the bank to ensure that keys of the godowns are held in dual custody, goods pledged to the bank tally with the record maintained in the Godown Register and the invoices both for quantity and value.
2. Verify if godown inspection is being conducted periodically and is properly recorded and reports thereof raised/submitted.
3. Verify if stock statements are being received at stipulated intervals, the statements are properly scrutinized drawing,

Training Material on Internal Audit

power is correctly calculated, DP Register is maintained and drawings/availments in the account so regulated.

4. Verify if all assets charged to the Bank are fully insured and Due Date Diary for insurance policies is maintained.
5. Verify whether lien is marked in the Register/Ledger against FDR/RD accounts against which advances have been granted and Deposit Receipts/ RD Passbooks are held duly discharged.
6. Verify whether NSCs/KVPs against which advance has been allowed have been pledged in favour of the Bank and the said lien notified to the concerned Post Office.
7. Checking of statements regarding limits sanctioned by the Branch Manager and statements regarding irregularity in the account permitted by the Branch Manager.
8. Verify the loans and advances allowed beyond the discretionary powers of the branch manager during the month and list such accounts along with date of regularization. Whether the same is reported in return to be submitted to higher authorities.
9. Verify if the letters of credit issued by the branch are within the delegated powers and ensure that they are for genuine transaction.
10. Verify Bank Guarantees - whether properly worded and recorded in the registers of the bank. Whether the extant guidelines are followed in issuance of Bank Guarantees.
11. Verify whether expired guarantees are surrendered back to the branch. In case of non returned expired guarantees, procedure as contained in HO circulars.
12. Proper follow up of overdue Bills/recourse to the drawers/merchandize etc.

13. Verify the limits / accounts falling due for review, renewal and the action taken by the branch on it. Verify whether Due Date, Diary of review/ renewal is maintained and required followup done on those dates.

Advances Under Consortium Arrangement

1. Guidelines contained in RBI directives and amended from time to time culminating into single window approach is followed.
2. Annual consortium meeting is held well in advance for the review of credit facilities. Likewise meetings of all consortium members are held whenever necessary to sort out problems, operational difficulties etc. if any. Generally a responsible officer who would take decision on behalf of the bank participates in such meetings. Minutes of the meeting are communicated to all consortium members. The branch keeps the controlling office informed of all the meetings and deliberations.
3. The lead bank and the next largest sharing bank meet at quarterly intervals to assess the performance of the borrower on the basis of the information under Quarterly Information System to fix operating limit/individual bank's shares for the next quarter and convey the same to all consortium members.
4. Joint inspections of the unit/stocks is carried out once a year and by individual banks at prescribed intervals as per arrangement and the reports are exchanged among the consortium members.
5. It is ensured that pro-rata business, including non-fund based business, is transacted through the participating banks.

Merchant Banking Business

1. Where the branch acts as a Collecting Branch for issue business, the instructions given by the Controlling Branch are properly followed.

Training Material on Internal Audit

2. The daily collection position is advised by telex to the Controlling Branch.
3. The funds are transferred to Short Deposit Account as instructed and particulars of individual Short Deposits are advised to the Controlling Branch.
4. Final Certificates are submitted properly and in time to the Controlling Branch.
5. The entire funds collected are remitted to the Controlling Branch, inclusive of amounts matured, the short deposits and interest thereon giving complete details of break-up of aggregate amount.
6. The branch does not accept applications from investors after the stipulated closing date of the issue.
7. Where the branch acts as a Controlling Branch, the terms and conditions on which the branch has accepted the role of Banker to the issue are complied with.
8. The branch is correctly recovering the commission and out-of-pocket expenses as agreed with the respective companies.
9. There is no delay in the issue of final certificates by the branch in its capacity as Controlling Branch.
10. Prescribed preventive vigilance measures are duly observed by the branch.
11. Where data entry or data processing work is entrusted to outside agencies, the competent authority duly approves these and the prescribed stamped indemnity has been obtained from such agencies.
12. It is ensured that dividend interest warrants/refund payment accounts of companies are funded prior to dispatch of the relative warrants by the companies and there is no misuse of the facility. Deviations, if any, have been made after obtaining the approval of the competent authority.

13. The branch is correctly recovering commission and out-of-pocket expenses from the concerned companies. The competent authority has duly authorized any waiver or reduction of such charges.
14. Claims for reimbursement of amounts of paid warrants received from paying branches are processed and debited to the concerned company's account promptly. Cases of inordinate delays in raising debits, if any, are mentioned.

Credit Card

1. Application for the issue of credit card has been properly examined and record of issue of the same has been maintained.
2. Ensure that the credit in respect of charge-slip is immediately given to the member establishment.
3. Ensure that the charge-slip is examined to verify that it does not cover any picked-up card.
4. Ensure that the debits arising out of the use of credit cards are promptly recovered.
5. The bank maintains a proper record of picked-up cards.
6. Undelivered credit cards are properly kept as security items and followed up with credit card department for further instructions.
7. Higher authorities are invariably informed about overdrafts/debits arising out of the use of credit cards.

VI. Foreign Exchange Including Export Finance

1. Verification regarding the reconciliation of NOSTRO and VOSTRO accounts and that balances in NOSTRO accounts are within the limit prescribed by the bank.
2. To monitor whether FEDAI rules have been observed in the extension and cancellation of forward contract - whether

Training Material on Internal Audit

competent authority scrutinizes them and the necessary charges, including delivery charges, have been recovered.

3. Levy of correct charges on foreign inward/outward remittances.
4. Monitor timely / proper submission of claims to ECGC.
5. Adherence to the guidelines issued by RBI/HO about dealing room operations.
6. Comment on irregularities in opening the accounts and operation in ordinary NR, FCNR NRE, EEFC and other nonresident accounts - whether the debits and credits are permissible under the rules.
7. All FCNR receipts are issued by the branch against consideration i.e. only after receipt of funds. High value deposits need special attention.
8. Whether rates quoted/applied by the branch on various types of purchase/ sale transactions are correct. Verify that over bought/over-sold position maintained in different currencies is reasonable taking into account foreign exchange operations as well as the extent up to which permission has been given to the branch by the International Division of Head Office for such positions.
9. Payment of ECGC Premium/Submission of required statements to ECGC for pre-shipment/post-shipment.
10. Submission of returns to RBI (R-return etc)
11. Verification of bill of entry and maintenance of proper records for it.
12. In respect of packing credits, please mention if there are overdues, whether they are covered by stocks, firm order or LCs, report to ECGC is made, premia paid, whether RBI's approval is sought. Whether claim is made with ECGC and followed up? Report details.

13. Whether commercial rate of interest is charged for overdue packing credits and those adjusted otherwise than by export bills.
14. Whether export bill purchased / negotiated / discounted is not realized on due date (in case of demand bills within Normal Transit Period and incase of usance bills on the notional due date) exporter's foreign exchange liability should be converted into Rupee liability on or before the 30th day from the notional due date at prevailing TT Selling Rate.
15. In case additional facility is given to exporter in the form of Pre-shipment credit in Foreign Currency (PLFC) or in the form of Rediscounting of Export bills abroad (EBRD) whether conditions applicable to these are complied with.

Note

- (i) Bank's manual of instructions on foreign exchange be stated.
- (ii) FEDAI rules? RBI circulars to be studied every month for any change / modification during the months.

VII. Refinance Management (IDBI/EXIM Bank/NABARD / SIDBI)

- (a) Whether all eligible term loans disbursed has been identified and reported without delay?
- (b) Whether the commercial rate of interest is charged till the date of refinance.
- (c) Eligible Term Loans, which were refinanced, should be reported.

VIII. Letter of Guarantee/Co Acceptance

Report on :

Irregularities in issue of guarantee

Training Material on Internal Audit

Invoked during the month

Expired during the month

Please specify clearly:

1. Whether it was issued as per the approved format/model guarantee prescribed and standard limitation clause is incorporated. Whether any onerous clause/unusual clause, which is impossible/difficult of compliance, is incorporated.
2. Whether counter indemnity is obtained as prescribed?
3. Any deviation from the terms of sanction in regard to margin, security, purpose, period, beneficiary, collection of charges, commission/fee etc.
4. Has the branch ensured that the claim is in order.
5. Has the branch been kept informed by the principal accountee and those liable under the counter-guarantee.
6. Have follow-up measures been taken as prescribed for the return of the original guarantee the validity period of which has already expired?
7. In respect of Deferred Payment Guarantee, whether payment is made to the debit of party's account on due date without creating overdraft/debiting suspense.

IX. Other Assets/Sundry Creditors / Accounts

1. Any outstanding in suspense/sundry debtors account outstanding for more than 15 days which is not of non recurring nature should be checked and commented for reasons of non adjustment.
2. Now most banks have service/link branches for pension payment/ reimbursement/ Govt. accounts transaction etc.
3. All PPO's are properly numbered and recorded.

4. Verify whether any excess pension is outstanding in branch for recovery.
5. Ensure whether link branch (if applicable) is sending pension payment scroll to RBI/SBI well in time for reimbursement.
6. Whether turnover commission is recovered by the link branch and distributed amongst branches.
7. Where reimbursement are in arrears.
8. Records at branch for pension payment (register are up to date).
9. For collection of taxes, PPF A/c etc whether funds received are immediately remitted to link branch.

X. Compliance of Guidelines on "Know Your Customer" Norms and "Cash Transactions" and Other Internal Control Measures

Whether bank has complied with the guidelines regarding cash transactions involving amount of Rs. 50,000/- while accepting the cash.

XI. Status of Implimentation of Mitra Committee Recommendations Relating to Submission of Legal Compliance Certificates

Check total no. of officers in the branch (excluding Branch Manager), of whom no of officers who have not submitted legal compliance certificate.

Whether the Branch Manager has submitted legal compliance certificate to his controlling office.

ANNEXURE - J

Checklist-Quarterly

I. Deposit

1. Verify interest paid in Savings Bank Account at random basis.
2. Verify interest provision in Term Deposit Accounts.
3. Balancing of 25% of SB ledgers, Current account ledgers other than term deposit registers should be verified in each quarter, so that all ledgers/ registers are covered during the year.

II. Advances

1. Verify whether the branch has correctly charged interest (including penal/ overdue interest), service charges, commission, discount, processing charges etc. on the loans and advances including Bills Purchased/ Discounted/Negotiated and Acceptances etc. at the stipulated rates and stipulated manner.
2. Verify proper classification of assets.
3. Verify whether operations in the accounts reveal any unhealthy features such as heavy withdrawals in cash, suggestive of diversion of funds for purposes other than the declared business of the borrowers.
4. Whether Select Operational Data and Quarterly Information System Statements in respect of big borrowers have been received promptly? Whether penal rate of interest @1 % is being charged for delayed submission / non-submission.
5. Verify whether the branch has charged lead bank charges in respect of advances under consortium norms.

III. House Keeping

1. Verify whether Accounts with HO are reconciled and old entries in HO accounts are reconciled and reversed.
2. Non-maintenance of registers, as required-is it maintenance or non-maintain.

IV. Revenue Checking

Verify and report non-recovery of:

- Locker rent
- Folio charges
- Penal interest for delayed/non-submission of returns, financial statement required to be submitted.
- Penal interest on advances in respect of lapsed sanction/limit
- Penal interest on excess over limit
- Overdue interest on all types of bills, loans and packing credits for overdue period
- Commitment fee for unutilised limit is collected as per rules.
- Commission of letter of credit, letter of guarantee and charges for safe custody etc.
- Standing information charges
- Stop payment charges
- Processing fee on advances
- Ledger folio charges

For rates, bank's service charges booklet/manual should be obtained and kept on record during the period of audit for any further clarification/ modification with effect as mentioned in respective circular are taken care of.

V. Computers

1. Number of computers in use.
2. Installed modules to be verified from Day Begin Operation Menu available for senior managers.
3. Hardware details such as brand name, hard disk capacity, processor name, from copy of invoices / copy of order that is available at branch.
4. AMC should be entered for all the system in use. The expiry date will be available from contract entered with vendor by the branch.
5. The name of printers, routers, and scanner, in use should also be stated.
6. UPS and AC details for brand, capacity, number of batteries.
7. Whether following registers are maintained and updated:
 - Computer, consumable maintenance log,
 - Computer cabin keys and their movement, and
 - Machine breakdowns/maintenance by vendor visits.
8. To check whether branch is changing the parameter whenever it is due, verify with respective maintenance options under module means.

ANNEXURE - K

Checklist-Half Yearly

1. Destruction of old records as per time schedule prescribed.
2. Proper maintenance of Security Personnel Register and Equitable Mortgage Register.
3. Incidental charges and service charges in Saving Bank Account (including inoperative) having balance below prescribed limit.
4. Concurrent Auditor should also comment on:
 - Availability of Power of Attorney of the signing Officers in the branch, staff strength, training, rotation of duties etc. to be checked.
 - 30% scrutiny of transactions relating to the payment of pension.
 - Whether the prescribed certificates - Life, Re-employment, Re-marriage etc. obtained, wherever required, in all pension accounts.
 - Physical checking of Govt. and other securities held on behalf of Investment Department and timely collection of interest thereon and their maturity proceeds.
5. Adequacy of the follow-up for realization of overdue export bills.
6. Compliance with insurance limit for cash and other fixed assets of branches.
7. Furniture and fixtures at branch are serially numbered and recorded in fixed assets register, are adequately insured. Depreciation is calculated at HO or branch wise.

Training Material on Internal Audit

8. If building is rented, rent agreement is kept in safe custody
9. Whether or not customer service is satisfactory, such as:
 - Customer meeting is convened once in quarter
 - Standing instructions are followed up
 - Complaint/suggestion box is there in branches
 - Whether or not staff at branch is polite to customers.

ANNEXURE - L

Security Verification

The asset checking during the Concurrent Audit has to be more extensive than during Regular Inspection. The Concurrent Auditor has to divide security checking in such a way that some of the borrower accounts are covered every month. More attention should be given to such accounts which are irregular or contain serious irregularities. The following frequency is to be observed:

S. No.	Fund Based Limit	Minimum Accounts to be covered every month	Minimum coverage during the year
1	Over Rs.10 Lacs*	20%	All accounts to be covered in each half year.
2	Rs.1 lac to Rs.10 lacs	10%	All accounts to be at least once in a year
3	Rs.25,000/- to Rs.1 lacs	2.5%	30% of loans and advances.
4	Upto Rs.25,000/-	One account	12 accounts

* While verifying securities in consortium advances, the system of securities checking prescribed in sanction may be taken into account and its adherence commented upon.

Stipulation laid down in sanctions regarding checking of stocks lying at outstation may be looked into and their adherence commented upon.

ANNEXURE - M

Computer Audit

1. Whether Server Room (in case of PBM/TBM branches) is locked overnight, kept neat and clean with air conditioner working perfectly.
2. Whether access to Server Room/computers/nodes/ ALPMs is restricted to authorised persons only.
3. In case of any breakdown, whether the same is noted in Machine Breakdown-cum-Vendor-Visit Register.
4. Verify whether UPS is working fine and in case of power failure, sufficient battery back up is available.
5. Verify that any other load (other than computer and peripherals) is not put on the UPS power points.
6. Whether back up is taken daily on floppy/cartridge tape/ other media by authorised official and are properly labelled with the days taken and date taken is noted on label outside.
7. Whether off-site storage of back-up of system and data are maintained?
8. Whether secrecy of passwords is maintained:
 - Whether passwords are changed periodically (verify whether periodical changes are recorded by mentioning the date of change of password).
 - Whether the user having only one user id.
9. Whether users the terminals without logging out? Whether operators are given access to DOS/UNIX prompt?
10. Whether any unauthorised software programmes are installed/used? If yes, collect details thereof.
11. Whether all balances are tallied with GL heads on day-to-

day basis.

12. Whether all transactions are authorised daily.
13. Whether signature scanning is done regularly for all newly-obtained signature cards.
14. Whether proper procedure is followed for data input and proper rubber stamp is affixed on the reverse of each voucher/data source and the same is filled up and initialed.
15. Whether latest anti-virus software has been installed.
16. Whether all reports/printouts are checked, signed by concerned official and filed properly.
17. Whether day book is prepared on the basis of checked final supplementary.
18. Whether summary balance report (fall back report) is taken and filed to meet contingency requirements.
19. Whether check sum is generated at day end and is tallied with that generated at next day begin and proper record of the same is maintained.
20. Whether or not any exceptional report is generated and checked by branch manger or not.

APPENDIX - N

Audit Programme of Concurrent Audit of Branch

1. Brief Profile of Branch

- (i) Name of Bank: Branch:
- (ii) Date of opening
- (iii) Branch code No.
- (iv) Name of Branch Manager Scale:
Since:
- (v) Branch category
 - (a) Operational Status Fully computerized
Partially computerized
Non-computerized
 - (b) Area wise Metropolitan/Urban/Rural
 - (c) Business wise Exceptional/Very
Large/Large/Small
- (vi) Name of Nodal officer at Branch
- (vii) Staff strength
 - (a) Officers
 - (b) Clerical
 - (c) Subordinate staff
 - (d) Part time

- (viii) Name of Extension Counter
- (ix) Bank premises Leased/owned
 - If leased
 - (a) Date of last lease deed
 - (b) Date of expiry of lease deed
- (x) Audit rating of branch
 - (a) Previous year
 - (b) Present
- (xi) Since when under concurrent audit

2. Appointment Letter No.

Period of assignment

Date of commencement

Date of submission of reports:

- Statutory audit report submitted on
- RBI inspection held on not at branch
- Previous concurrent audit report submitted on
- Present month wise status of report submission to be given as under Month Date of submission

3. Audit in charge

Audit assistants

4. Guidelines / instructions: At the time of starting of audit the following instructions may be taken care of:

- i) Audit- in- charge along with assistant to have a formal introduction with branch manager. Then along with

him or with Nodal officer he should have introduction with branch staff. This is necessary because the concurrent audit is day-to-day audit and auditor has to visit every department of branch.

- ii) Get and held on record a copy of scope of work and reporting requirement of concerned bank
- iii) To effectively carry out the audit it is necessary to be familiar with:
 - (a) Circulars from head office.
 - (b) Terminologies used by bank to describe transactions as different bank used different terms to describe a transaction though the methodology of transaction remains same.
 - (c) Accounting and Auditing Standards i.e. applicability of the accounting standards and auditing assurance statements issued by ICAI at the branch. For this it would be better to go through the previous statutory audit report and tax audit report of branch. Auditor should follow the auditing assurance statements while conducting the audit.
 - (d) That the procedural aspect of a transaction is given in the Documentation Manual of respective banks and one latest copy of these manuals is available at branch. Auditor should refer and follow instructions mentioned in these manuals.
 - (e) Internal controls at branch, initially the Concurrent Auditor should observe a set of transactions in details to judge whether the internal controls at different department is adequate or not. In case he is not convinced with this he should define remedial procedures to improve these controls.
- iv) Auditor should conduct audit of various transactions as per frequency mentioned in checklists given in Annexures.

- (v) A daily record in the form of a register must be kept of all queries made and responses received. This register to be signed by auditor and the concerned person who have responded against the queries as a confirmation of audit communication made.
- (vi) The audit procedures outlined in the checklists (in Annexures) are the minimum, have been prepared head wise and must be followed. Audit procedures recommended may be strengthened in areas of weaknesses and additional procedures added to the audit programme.

MODULE - VIII

INTERNAL AUDIT AND CORPORATE GOVERNANCE

Chapter-VIII.1

Corporate Governance - An Overview

Corporate Governance

1. Corporate governance, in the simplest terms, refers to the systems by which companies are directed and controlled. Governance is the structure used by the management to oversee the activities of the organisations. Research has shown that companies having good corporate governance practices in place are remunerated in the form of better prices of their securities, easier access to capital, reduced cost of capital, better ability to attract and retain talent, better utilization of resources, etc. The importance of corporate governance, thus, cannot be over-emphasized. Corporate governance has also emerged a strong tool in the hands of the regulators for protecting the interests of the investors. Thus, over a period of time, the Governments and regulators, both at home and abroad, have issued comprehensive laws and regulations in respect of model corporate governance practices to be adopted by the companies.

There has been renewed interest in the corporate governance practices of modern corporations since 2001, particularly due to the high-profile collapses of a number of large U.S. firms such as Enron Corporation and Worldcom. In 2002, the US federal government passed the Sarbanes-Oxley Act, intending to restore public confidence in corporate governance.

Corporate governance activities are represented as four principal components:

- **Rights and equitable treatment of shareholders:** Organizations should respect the rights of shareholders and help shareholders to exercise those rights. They can help shareholders exercise their rights by effectively communicating information that is understandable and

accessible and encouraging shareholders to participate in general meetings.

- **Interests of other stakeholders:** Organizations should recognize that they have legal and other obligations to all legitimate stakeholders.
- **Role and responsibilities of the board:** The board needs a range of skills and understanding to be able to deal with various business issues and have the ability to review and challenge management performance. It needs to be of sufficient size and have an appropriate level of commitment to fulfill its responsibilities and duties.
- **Integrity and ethical behaviour:** Ethical and responsible decision making is not only important for public relations, but it is also a necessary element in risk management and avoiding lawsuits. Organizations should develop a code of conduct for their directors and executives that promotes ethical and responsible decision making.
- **Disclosure and transparency:** Organizations should clarify and make publicly known the roles and responsibilities of board and management to provide shareholders with a level of accountability. They should also implement procedures to independently verify and safeguard the integrity of the company's financial reporting. Disclosure of material matters concerning the organization should be timely and balanced to ensure that all investors have access to clear, factual information.

Participants in Corporate Governance

Following participate in corporate governance:

1. the Board of Directors
2. the Management
3. the Audit Committee
4. the Stakeholders including shareholders, suppliers, customers, employees etc.

The Board of Directors

The Board of Directors as well as its members individually plays an important role in corporate governance process. The Board is responsible for the oversight of all matters of the corporate governance. The board of directors thus should provide governance, guidance, and oversight to senior management. It is ultimately responsible for ensuring that an appropriate internal control system is in place, including risk assessment. The overall responsibilities of the Board includes the following:

1. Assessing the scope and effectiveness of the systems established by management to identify, assess, manage and monitor the various risks arising from the organisations activities.
2. Ensuring the management establishes and maintains adequate and effective internal controls.
3. Satisfying that appropriate controls are in place for monitoring compliance with laws, regulations, supervisory requirements, and relevant internal policies.
4. Monitoring and reviewing the effectiveness of internal audit function.
5. Communication and disclosure- financial and operational.

Audit Committee

Audit Committees are vital to investors and internal auditors. For the investor, they have to provide confidence in corporate governance. For internal auditor, they have to assure his independence. The responsibility of audit committees in the area of corporate governance is to provide assurance that the corporation is reasonably complying with pertinent laws and regulations and is conducting its affairs effectively and is maintaining effective controls.

Management

The management deals with all aspects of corporate governance on day-to-day basis. Within the management, a particular importance is given to the Chief Executive Officer (CEO). CEOs are the most important players in the internal control oversight process that add the best value. The overall responsibilities of the Management includes the following:

1. Internal controls relating to financial reporting are adequately designed and operating.
2. Management is required to demonstrate that for key elements of the financial statements, there are adequate controls built into the underlying processes to ensure reliable financial reporting.
3. Management is able to demonstrate, by a process of verification that the controls built are operating throughout the year.

Stakeholders

Stakeholders mainly include investors (shareholders, financiers-banks, creditors, etc.), employees, suppliers, and customers. The challenges for corporate governance is to meet the expectations of both the stakeholders and the shareholders, for an organisation cannot be successful while neglecting the expectations and needs of either.

Importance of Corporate Governance matters

It is essential to understand the importance of corporate governance. The corporate governance has the impact on:

1. efficient use of resources
2. ability to attract low-cost capital
3. ability to meet societal expectations
4. overall performance

1. *Efficient use of resources*

Effective corporate governance promotes the efficient use of resources since organization who actually exercise good and effective corporate governance will also attract investors capital. Indeed, through exercising good corporate governance those organizations will prove to the potential shareholders their capability of producing goods or services in the most 'efficient' way and at the same time yielding a high return.

2. *Ability to attract low-cost capital*

The procedure for corporate governance also include the procedures which will protect the amount invested in shares by the investors. This in turn would increase the investors' confidence that would lead to low-cost capital.

These procedures applied to protect the shares should include:

- independent monitoring of management,
- transparency in corporate performance,
- ownership and control, and
- possibility to participate in certain fundamental decisions.

Moreover, the investor is prepared to pay more for a company with good corporate governance because:

1. he believes that the company will perform better in the future.
2. he believes he is reducing risk.
3. the attention devoted to corporate governance is a fad and one does not want to be left behind (everybody does it).

3. *Ability to meet social expectations*

Ability to meet social expectations means governance of internal controls, compliance with the laws and regulations.

4. Overall performance

Taking into account the first three impact factors, the only thing still missing for the overall performance is the accountability by the board and management. Corporate governance as such is no guarantee for improved success. It should, however, contribute to a more efficient use of assets, to attracting low-cost capital, to meeting expectations of stakeholders and shareholders, to helping to avoid or prevent corruption within the organization, and in doing so lead to enhanced (better) performance.

Chapter-VIII.2

Impact of Corporate Governance Requirements on Internal Audit

Internal control provides some degree of assurance for the achievement of corporate objectives, and an important part of every internal audit function is how control and governance integrate in the audit environment. Current thinking on corporate governance dictates that the effectiveness of internal auditing depends on its place in the organisation and the use of professional staff together with the use of recognised internal auditing standards. Historically, due to the growing complexity and expansion of organisations, management needed to control business processes. The consequence was that internal auditors needed to concentrate on the way business controls were managed, moving from the traditional financial audits, which were transferred to some extent to line managers and external auditors.

Clause 49 of the Listing Agreement

In India, introduction of clause 49 in the Listing Agreement issued by the Securities and Exchange Board of India (SEBI) has had a significant role to play in shaping the face of the corporate governance practices in listed companies in India. The provisions of the revised Clause 49 were to be implemented as per the following implementation schedule:

- a) For entities seeking listing for the first time, at the time of seeking in-principle approval for such listing.
- b) For existing listed entities which were required to comply with the erstwhile clause 49 (i.e., those having a paid up share capital of Rs. 30 million and above or net worth of Rs. 250 million or more at any time in the history of company), by April 1, 2005

Training Material on Internal Audit

Some of the important requirements of clause 49 are as follows:

- Companies need to submit a quarterly report in respect of compliance with clause 49 of the Listing Agreement to the stock exchanges within the stipulated time from the close of quarter signed by the Compliance Officer or the Chief Executive Officer.
- The Audit Committees are required to review:
 - The adequacy of the internal audit function, if any, including the structure of internal audit department, staffing and seniority of the official heading the department, reporting structure coverage and frequency of internal audit, including appointment, removal and terms of remuneration of the chief internal auditor.
 - Internal audit reports relating to internal control weaknesses.
 - The findings of any internal investigations by the internal auditors into matters where there is a suspected fraud or irregularity or a failure of internal control systems of a material nature and reporting the matter to the Board.
- The Audit Committee is also required to discuss with the internal auditors any significant findings and follow up thereon.
- The CEO and the CFO is required to certify to the Board of Directors:
 - That financial statements as well as the cash flow statement for the period:
 - Do not contain any materially untrue statement or omit any material fact or contain statements that might be misleading.
 - Present a true and fair view.
 - Are in compliance with the existing Accounting Standards, applicable laws and regulations.

Impact of Corporate Governance Requirements on Internal Audit

- No transactions were entered into by the company, which were fraudulent, illegal or violative of the company's code of conduct.
- That they accept responsibility for effectiveness of internal controls and that they have disclosed to the auditors and the Audit Committee deficiencies in the design and operation of the internal controls and steps taken for rectification of the same.
- That they have indicated to the Audit Committee and the internal as well as external auditors as to the following aspects:
 - Any significant changes in internal controls.
 - Any significant changes in the accounting policies and instances of significant fraud, if any, and that the same have been disclosed in the notes to the financial statements.
 - Instances of any significant fraud and involvement, if any, therein of the management or any employee having a significant role in the internal control systems of the company.

Thus, it is amply evident from the above that the management, especially the functional management as well as the Audit Committee needs extensive support from the internal audit function to give it the primary assurance about controls and compliances before giving the required reports/certificates or to appropriately review the necessary aspects and make informed decisions. The complete text of the clause 49 of the Listing Agreement is enclosed as **APPENDIX I**.

Section 292A of the Companies Act, 1956

In addition, section 292A of the Companies Act, 1956, requires public companies having paid up capital not less than Rs. Five crores to constitute a committee of the Board i.e., the Audit Committee. In terms of sub section (5) of the said section, the internal auditor is required to attend and participate at the

meetings of such Audit Committees. Thus, by implication, section 292A also lays down the requirement for internal audit to the companies falling under the purview of section 292A of the said Act.

Companies (Auditor's Report) Order, 2003

The importance of internal audit to the corporate enterprises was recognized by the Government way back in 1975 under the Companies Act, 1956 itself. The Manufacturing and Other Companies (Auditor's Report) Order 1975 issued by the Central Government in terms of section 227(4A) of the Companies Act, 1956 required the statutory auditor to report whether, in relation to companies the paid-up capital of which at the commencement of the financial year concerned exceeded Rs.25 lakh, the company had an internal audit system commensurate with its size and nature of its business. This implied requirement for internal audit was kept intact in the 1988 Order as well except that an additional condition of turnover of Rs. 2 crores for three consecutive years was introduced. The Central Government, in terms of the power vested under section 227(4A) of the Companies Act, 1956, in June 12, 2003, had notified the Companies (Auditor's Report) Order, 2003. Clause (vii) of the said 2003 Order requires the auditor to report as follows:

“whether in case of listed companies and/ or other companies having paid-up capital and reserves exceeding Rs. 50 lakh at the commencement of the financial year concerned, or having an average annual turnover exceeding five crore rupees for a period of three consecutive financial years immediately preceding the financial year concerned, whether the company has an internal audit system commensurate with its size and nature of its business.”

Though the clause does not by itself mandate internal audit in the subjected companies, yet a company to which the same is applicable, would incur a negative remark from the auditor if it does not have an internal audit system.

In addition to the requirement to comply with the provisions of clause 49 of the Listing Agreement or the Companies Act, 1956,

Impact of Corporate Governance Requirements on Internal Audit

as mentioned above, companies going in for tapping the international capital market, especially, those seeking listing in US stock exchanges, NASDAQ, NYSE etc., also need a strong internal audit function to meet the stringent corporate governance and internal control requirements of those stock exchanges. In this context, the US companies, having US public as investor also needs to comply with the requirements of section 302 and 404 of the Sarbanes Oxley Act of 2002.

Chapter-VIII.3

Role of Internal Audit in Strengthening Corporate Governance

Implementation of corporate governance practices involves certain costs to be incurred by the company. The company needs to justify the cost of implementing good corporate governance principles *vis-a-vis* benefits derived therefrom. Internal audit can help maximizing the benefits from the corporate governance policies. Preface to the Standards on Internal Audit describes internal audit as *“an independent function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system.”* It makes clear that internal audit involves critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system.

The internal audit activity also includes the evaluation and provide suggestions for improvements of risk management, internal control systems and overall governance mechanism. It is a systematic evaluation of risk management, control and governance processes particularly with reference to:

- Safeguarding of assets.
- Compliance with laws, regulations and contracts as well as policies laid down by the management.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations.

Role of Internal Audit in Strengthening Corporate Governance

- Accomplishment of objectives and goals of the organization through ethical and effective governance.

Following are some of the measures by which internal audit contributes to sound corporate governance:

- (i) Understanding and assessing the risks and evaluate the adequacies of the prevalent internal controls.
- (ii) Identifying areas for systems improvement and strengthening controls.
- (iii) Ensuring optimum utilization of the resources of the entity, for example, human resources, physical resources, etc.
- (iv) Ensuring proper and timely identification of liabilities, including contingent liabilities of the entity.
- (v) Ensuring compliance with internal and external guidelines and policies of the entity as well as the applicable statutory and regulatory requirements.
- (vi) Safeguarding the assets of the entity.
- (vii) Reviewing and ensuring adequacy of information systems security and control.
- (viii) Reviewing and ensuring adequacy, relevance, reliability, and timeliness of management information system.

Chapter-VIII.4

Relationship Between the Audit Committee and Internal Auditor

The internal audit function is a major source of information and assurance to the Audit Committee on internal controls and other risk management activities. It is for this reason that the internal audit team should have functional reporting responsibilities to the Audit Committee as defined in the internal audit charter.

Both the internal audit and Audit Committee charters should clearly state that:

- The Chief Internal Auditor would have direct and unrestricted access to the Chairman of the Audit Committee.
- The Chief Internal Auditor would attend and participate in the meetings of the Audit Committee to present the internal audit plan for the period and to report the internal audit findings.
- The Audit Committee would review and approve the appointment/replacement of the chief internal auditor.
- The internal audit charter would be reviewed by the Audit Committee periodically.
- Internal auditor would provide the Audit Committee members and senior management with independent, objective views on risk and internal controls within the enterprise.
- Where internal audit function is outsourced, the outside agency should nominate its senior personnel who should report to the Audit Committee. Where more than one such agency is involved, each should nominate its senior

Relationship Between the Audit Committee and Internal Auditor

personnel for this purpose. Where outside agency/ies are involved, a senior internal manager would be nominated to co-ordinate the internal audit function.

The Audit Committee should be responsible for confirming that internal audit has the competence, independence, resources and corporate support to do its job properly, and is demonstratively effective in getting results.

Chapter-VIII.5

Relationship Between the Board of Directors and Internal Auditor

The Chairman of the Audit Committee, when reporting to the Board, should include the recommendations of the Audit Committee as to the effectiveness, capabilities, findings and concerns of the internal auditor.

The internal audit plays a key role in supporting the board in ensuring adequate oversight of internal controls and in doing so form an integral part of an organisation's corporate governance framework.

The key role played by the internal auditor in assisting the board in discharging its governance responsibilities are as follows:

1. A review of the organisation's control system.
2. An objective evaluation of existing risk and internal control framework.
3. Systematic analysis of business processes and associated controls.
4. Reviews of existence and value of assets.
5. Provide information on major frauds and irregularities.
6. Reviews of compliance framework.
7. Reviews of operational and financial performance.
8. Recommendations for more effective and efficient use of resources.
9. Assessments of accomplishments of corporate goals and objectives.

Chapter-VIII.6

Corporate Governance and Internal Control

Clause 49 of the Listing Agreement has been an important instrument in promoting and strengthening sound governance practices in the companies listed on the recognised stock exchanges in India. From time to time the clause has been revised to not only reflect the growing expectations of the investors as well as the regulators from the listed companies, changes in local laws and regulations but also to help the Indian companies, now spreading wings in even the most developed international economies, benchmark with the international governance best practices. In this line, the clause 49 was revised by the Securities and Exchange Board of India (SEBI) vide its circular No. SEBI/CFD/DIL/CG/1/2004/12/10 dated October 29, 2004.

The revised clause 49 requires the Chief Executive Officer (CEO)/ Chief Financial Officer (CFO) of a listed company to certify their responsibility for and continued existence and operation of ***internal controls*** in the company. They are also required to certify that they had disclosed any deficiency in the design or operation of internal controls to the audit committee and the auditor and that adequate steps have been taken to do away that deficiency.

Though the abovementioned requirements of the so revised clause 49 were apparently analogous to the similar requirements of section 404 of the Sarbanes Oxley Act of 2002 in existence in the United States of America, there was a significant and critical difference between the two. Whereas the revised clause 49 envisaged the CEO/ CFO certificate in respect of the entire system of internal controls in the company, section 404 envisaged the same only in respect of internal controls over financial reporting. The provisions of revised clause 49 were, therefore, much larger in scope. SEBI, however, vide its another circular No.

Training Material on Internal Audit

SEBI/CFD/DIL/CG/1/2006/13 dated January 13, 2006) did away with the anomaly as follows:

“The CEO, i.e. the Managing Director or Manager appointed in terms of the Companies Act, 1956 and the CFO i.e. the whole-time Finance Director or any other person heading the finance function discharging that function shall certify to the Board that:

- a) They have reviewed financial statements and the cash flow statement for the year and that to the best of their knowledge and belief :
 - i. These statements do not contain any materially untrue statement or omit any material fact or contain statements that might be misleading; and
 - ii. These statements together present a true and fair view of the company's affairs and are in compliance with existing accounting standards, applicable laws and regulations.
- b) There are, to the best of their knowledge and belief, no transactions entered into by the company during the year which are fraudulent, illegal or violative of the company's code of conduct.
- c) They accept responsibility for establishing and maintaining internal controls for financial reporting and that they have evaluated the ***effectiveness of the internal control systems of the company pertaining to financial reporting*** and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of such internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies. (emphasis added).
- d) They have indicated to the auditors and the Audit committee:
 - i. Significant changes in internal control over financial reporting during the year;

- ii. Significant changes in accounting policies during the year and that the same have been disclosed in the notes to the financial statements; and
- iii. Instances of significant fraud of which they have become aware and the involvement therein, if any, of the management or an employee having a significant role in the company's internal control system over financial reporting.”

Components of Internal Control

Internal control comprises of five interrelated components as follows:

- a) Control Environment
- b) Entity's Risk Assessment Process
- c) Information and Communication
- d) Control Activities and
- e) Monitoring.

The Guide to Internal Controls Over Financial Reporting issued by the Internal Audit Standards Board* provides guidance in respect of sub clauses c and d above as they relate to establishment and assessment of internal controls over financial reporting.

* Hitherto known on Committee on Internal Audit

Chapter-VIII.7

Risk Management

With the large number of corporate scandals rocking the corporate world with the turn of the century, the concept of enterprise risk management has gained immense importance. As the name suggests, risk management refers to methods and processes used by organizations to manage risks (or seize opportunities) related to the achievement of their objectives. Risk management covers all categories and all material risk factors that can influence the organization's value.

Risks are continuously changing along with the environmental around and hence risk management is a continuous and cyclical process. The organisation's management is responsible for risk management across the organisation which is five step process; planning for risk and setting the objectives of risk management, risk identification, risk impact analysis- evaluation or estimation, risk strategy and risk monitoring. Internal auditors concentrates on riskier areas of the organisation, its approach is based on the assessment of risk. It audits the risk management process built by the management and ensures that the audit resources are utilised towards assessing the management of most significant risks. Internal auditors mainly focus on ensuring the effectiveness of controls, which treat risks. Internal Auditors notice the following subtle differences during such assignment:

- Shift of focus from reviewing controls to reviewing risk.
- Extensive preparation required on understanding the macro economics of the industry, the positioning of the organisation, its objectives, strategies and processes.
- Significant coverage of risks which are externally driven.
- Increased dependence on risk management documentation which links objectives, processes, risks, controls, and people.

In this regard, internal auditors carry out following activities:

- Understanding the risk maturity through discussions and documents.
- Drawn conclusion on risk maturity.
- Deciding on the audit strategy.
- Categorizing and prioritizing the risk.
- Allocating resources.
- Carrying out audit procedures on monitoring controls.
- Reporting and feed back on action taken.

Internal audit reports may include the following:

- Assessment of the risk maturity levels, both at the organisational and assignment level.
- Opinion on whether the laid down risk management policies and framework are being followed.
- Opinion on whether the laid down risk assessment processes are adequate and are being followed.
- Report on whether there are error indicators relating to management estimates on risks.
- Assessment on control scores and an opinion on the residual score of risks in the audit plan.

Chapter-VIII.8

Clause 49 - Corporate Governance

The company agrees to comply with the following provisions:

I. Board of Directors

(A) Composition of Board

- (i) The Board of directors of the company shall have an optimum combination of executive and non-executive directors with not less than fifty percent of the board of directors comprising of non-executive directors.
- (ii) Where the Chairman of the Board is a non-executive director, at least one-third of the Board should comprise of independent directors and in case he is an executive director, at least half of the Board should comprise of independent directors.
- (iii) For the purpose of the sub-clause (ii), the expression 'independent director' shall mean a non-executive director of the company who:
 - a. apart from receiving director's remuneration, does not have any material pecuniary relationships or transactions with the company, its promoters, its directors, its senior management or its holding company, its subsidiaries and associates which may affect independence of the director;
 - b. is not related to promoters or persons occupying management positions at the board level or at one level below the board;

- c. has not been an executive of the company in the immediately preceding three financial years;
- d. is not a partner or an executive or was not partner or an executive during the preceding three years, of any of the following:
 - i) the statutory audit firm or the internal audit firm that is associated with the company, and
 - ii) the legal firm(s) and consulting firm(s) that have a material association with the company.
- e. is not a material supplier, service provider or customer or a lessor or lessee of the company, which may affect independence of the director; and
- f. is not a substantial shareholder of the company i.e. owning two percent or more of the block of voting shares.

Explanation

For the purposes of the sub-clause (iii):

- a. Associate shall mean a company which is an “associate” as defined in Accounting Standard (AS) 23, “Accounting for Investments in Associates in Consolidated Financial Statements”, issued by the Institute of Chartered Accountants of India.
- b. “Senior management” shall mean personnel of the company who are members of its core management team excluding Board of Directors. Normally, this would comprise all members of management one level below the executive directors, including all functional heads.
- c. “Relative” shall mean “relative” as defined in section 2(41) and section 6 read with schedule IA of the Companies Act, 1956.

- (iv) Nominee directors appointed by an institution which has invested in or lent to the company shall be deemed to be independent directors.

Explanation:

“Institution’ for this purpose means a public financial institution as defined in Section 4A of the Companies Act, 1956 or a “corresponding new bank” as defined in section 2(d) of the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970 or the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980 [both Acts].”

(B) Non executive directors’ compensation and disclosures

All fees/compensation, if any paid to non-executive directors, including independent directors, shall be fixed by the Board of Directors and shall require previous approval of shareholders in general meeting. The shareholders’ resolution shall specify the limits for the maximum number of stock options that can be granted to non-executive directors, including independent directors, in any financial year and in aggregate.

(C) Other provisions as to Board and Committees

- (i) The board shall meet at least four times a year, with a maximum time gap of three months between any two meetings. The minimum information to be made available to the board is given in **Annexure– I A**.
- (ii) A director shall not be a member in more than 10 committees or act as Chairman of more than five committees across all companies in which he is a director. Furthermore it should be a mandatory annual requirement for every director to inform the company about the committee positions he occupies in other companies and notify changes as and when they take place.

Explanation:

1. For the purpose of considering the limit of the committees on which a director can serve, all public limited companies, whether listed or not, shall be included and all other companies including private limited companies, foreign companies and companies under Section 25 of the Companies Act shall be excluded.
 2. For the purpose of reckoning the limit under this sub-clause, Chairmanship/ membership of the Audit Committee and the Shareholders' Grievance Committee alone shall be considered.
- (iii) The Board shall periodically review compliance reports of all laws applicable to the company, prepared by the company as well as steps taken by the company to rectify instances of non-compliances.

(D) Code of Conduct

- (i) The Board shall lay down a code of conduct for all Board members and senior management of the company. The code of conduct shall be posted on the website of the company.
- (ii) All Board members and senior management personnel shall affirm compliance with the code on an annual basis. The Annual Report of the company shall contain a declaration to this effect signed by the CEO.

Explanation:

For this purpose, the term "senior management" shall mean personnel of the company who are members of its core management team excluding Board of Directors.. Normally, this would comprise all members of management one level below the executive directors, including all functional heads.

II Audit Committee

(A) Qualified and Independent Audit Committee

A qualified and independent audit committee shall be set up, giving the terms of reference subject to the following:

- (i) The audit committee shall have minimum three directors as members. Two-thirds of the members of audit committee shall be independent directors;
- (ii) All members of audit committee shall be financially literate and at least one member shall have accounting or related financial management expertise;

Explanation :

- 1. The term “financially literate” means the ability to read and understand basic financial statements i.e. balance sheet, profit and loss account, and statement of cash flows.
 - 2. A member will be considered to have accounting or related financial management expertise if he or she possesses experience in finance or accounting, or requisite professional certification in accounting, or any other comparable experience or background which results in the individual’s financial sophistication, including being or having been a chief executive officer, chief financial officer or other senior officer with financial oversight responsibilities.
- (iii) The Chairman of the Audit Committee shall be an independent director;
 - (iv) The Chairman of the Audit Committee shall be present at Annual General Meeting to answer shareholder queries;
 - (v) The audit committee may invite such of the executives, as it considers appropriate (and particularly the head of the finance function) to be present at the meetings of the committee, but on occasions it may also meet without the presence of any executives of the company. The finance director, head of internal audit and a representative of the

statutory auditor may be present as invitees for the meetings of the audit committee; and

- (vi) The Company Secretary shall act as the secretary to the committee.

(B) Meeting of Audit Committee

The audit committee should meet at least four times in a year and not more than four months shall elapse between two meetings. The quorum shall be either two members or one third of the members of the audit committee whichever is greater, but there should be a minimum of two independent members present.

(C) Powers of Audit Committee

The audit committee shall have powers, which should include the following:

1. To investigate any activity within its terms of reference.
2. To seek information from any employee.
3. To obtain outside legal or other professional advice.
4. To secure attendance of outsiders with relevant expertise, if it considers necessary.

(D) Role of Audit Committee

The role of the audit committee shall include the following:

1. Oversight of the company's financial reporting process and the disclosure of its financial information to ensure that the financial statement is correct, sufficient and credible.
2. Recommending to the Board, the appointment, re-appointment and, if required, the replacement or removal of the statutory auditor and the fixation of audit fees.
3. Approval of payment to statutory auditors for any other services rendered by the statutory auditors.

Training Material on Internal Audit

4. Reviewing, with the management, the annual financial statements before submission to the board for approval, with particular reference to:
 - a. Matters required to be included in the Director's Responsibility Statement to be included in the Board's report in terms of clause (2AA) of section 217 of the Companies Act, 1956.
 - b. Changes, if any, in accounting policies and practices and reasons for the same.
 - c. Major accounting entries involving estimates based on the exercise of judgment by management.
 - d. Significant adjustments made in the financial statements arising out of audit findings.
 - e. Compliance with listing and other legal requirements relating to financial statements.
 - f. Disclosure of any related party transactions g. Qualifications in the draft audit report.
5. Reviewing, with the management, the quarterly financial statements before submission to the board for approval.
6. Reviewing, with the management, performance of statutory and internal auditors, adequacy of the internal control systems.
7. Reviewing the adequacy of internal audit function, if any, including the structure of the internal audit department, staffing and seniority of the official heading the department, reporting structure coverage and frequency of internal audit.
8. Discussion with internal auditors any significant findings and follow up there on.
9. Reviewing the findings of any internal investigations by the internal auditors into matters where there is suspected fraud or irregularity or a failure of internal control systems of

a material nature and reporting the matter to the board.

10. Discussion with statutory auditors before the audit commences , about the nature and scope of audit as well as post-audit discussion to ascertain any area of concern.
11. To look into the reasons for substantial defaults in the payment to the depositors, debenture holders, shareholders (in case of non payment of declared dividends) and creditors.
12. To review the functioning of the Whistle Blower mechanism, in case the same is existing.
13. Carrying out any other function as is mentioned in the terms of reference of the Audit Committee.

Explanation :

- (i) The term "related party transactions" shall have the same meaning as contained in the Accounting Standard 18, Related Party Transactions, issued by The Institute of Chartered Accountants of India.
- (ii) If the company has set up an audit committee pursuant to provision of the Companies Act, the said audit committee shall have such additional functions / features as is contained in this clause.

(E) Review of information by Audit Committee

The Audit Committee shall mandatorily review the following information:

1. Management discussion and analysis of financial condition and results of operations;
2. Statement of significant related party transactions (as defined by the audit committee), submitted by management;
3. Management letters / letters of internal control weaknesses

issued by the statutory auditors;

4. Internal audit reports relating to internal control weaknesses; and
5. The appointment, removal and terms of remuneration of the Chief internal auditor shall be subject to review by the Audit Committee

III. Subsidiary Companies

1. At least one independent director on the Board of Directors of the holding company shall be a director on the Board of Directors of a material non listed Indian subsidiary company.
2. The Audit Committee of the listed holding company shall also review the financial statements, in particular, the investments made by the unlisted subsidiary company.
3. The minutes of the Board meetings of the unlisted subsidiary company shall be placed at the Board meeting of the listed holding company. The management should periodically bring to the attention of the Board of Directors of the listed holding company, a statement of all significant transactions and arrangements entered into by the unlisted subsidiary company.

Explanation :

- (i) The term “material non-listed Indian subsidiary” shall mean an unlisted subsidiary, incorporated in India, whose turnover or net worth (i.e. paid up capital and free reserves) exceeds 20% of the consolidated turnover or net worth respectively, of the listed holding company and its subsidiaries in the immediately preceding accounting year.
- (ii) The term “significant transaction or arrangement” shall mean any individual transaction or arrangement that exceeds or is likely to exceed 10% of the total revenues or total expenses or total assets or total liabilities, as the case may be, of the material unlisted subsidiary for the immediately preceding accounting year.

- (iii) Where a listed holding company has a listed subsidiary which is itself a holding company, the above provisions shall apply to the listed subsidiary insofar as its subsidiaries are concerned.

IV. Disclosures

(A) Basis of related party transactions

- (i) A statement in summary form of transactions with related parties in the ordinary course of business shall be placed periodical ly before the audit committee.
- (ii) Details of m aterial individual transactions with related parties which are not in the normal course of business shall be placed before the audit committee.
- (iii) Details of material individual transactions with related parties or others, which are not on an arm's length basis should be placed before the audit committee, together with Management's justification for the same.

(B) Disclosure of Accounting Treatment

Where in the preparation of financial statements, a treatment different from that prescribed in an Accounting Standard has been followed, the fact shall be disclosed in the financial statements, together with the management's explanation as to why it believes such alternative treatment is more representative of the true and fair view of the underlying business transaction in the Corporate Governance Report.

(C) Board Disclosures – Risk management

The company shall lay down procedures to inform Board members about the risk assessment and minimization procedur es. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework.

(D) Proceeds from public issues, rights issues, preferential issues etc.

When money is raised through an issue (public issues, rights issues, preferential issues etc.), it shall disclose to the Audit Committee, the uses / applications of funds by major category (capital expenditure, sales and marketing, working capital, etc), on a quarterly basis as a part of their quarterly declaration of financial results. Further, on an annual basis, the company shall prepare a statement of funds utilized for purposes other than those stated in the offer document/prospectus /notice and place it before the audit committee. Such disclosure shall be made only till such time that the full money raised through the issue has been fully spent. This statement shall be certified by the statutory auditors of the company. The audit committee shall make appropriate recommendations to the Board to take up steps in this matter.

(E) Remuneration of Directors

- (i) All pecuniary relationship or transactions of the non-executive directors *vis-à-vis* the company shall be disclosed in the Annual Report.
- (ii) Further the following disclosures on the remuneration of directors shall be made in the section on the corporate governance of the Annual Report :
 - (a) All elements of remuneration package of individual directors summarized under major groups, such as salary, benefits, bonuses, stock options, pension etc.
 - (b) Details of fixed component and performance linked incentives, along with the performance criteria.
 - (c) Service contracts, notice period, severance fees.
 - (d) Stock option details, if any – and whether issued at a discount as well as the period over which accrued and over which exercisable.

- (iii) The company shall publish its criteria of making payments to non-executive directors in its annual report. Alternatively, this may be put up on the company's website and reference drawn thereto in the annual report.
- (iv) The company shall disclose the number of shares and convertible instruments held by non-executive directors in the annual report.
- (v) Non-executive directors shall be required to disclose their shareholding (both own or held by / for other persons on a beneficial basis) in the listed company in which they are proposed to be appointed as directors, prior to their appointment. These details should be disclosed in the notice to the general meeting called for appointment of such director.

(F) Management

- (i) As part of the directors' report or as an addition thereto, a Management Discussion and Analysis report should form part of the Annual Report to the shareholders. This Management Discussion and Analysis should include discussion on the following matters within the limits set by the company's competitive position:
 - i. Industry structure and developments.
 - ii. Opportunities and Threats.
 - iii. Segment-wise or product-wise performance.
 - iv. Outlook.
 - v. Risks and concerns.
 - vi. Internal control systems and their adequacy.
 - vii. Discussion on financial performance with respect to operational performance.
 - viii. Material developments in Human Resources / Industrial Relations front, including number of people employed.

- (ii) Senior management shall make disclosures to the board relating to all material financial and commercial transactions, where they have personal interest, that may have a potential conflict with the interest of the company at large (for e.g. dealing in company shares, commercial dealings with bodies, which have shareholding of management and their relatives etc.).

Explanation:

For this purpose, the term "*senior management*" shall mean personnel of the company who are members of its core management team excluding the Board of Directors). This would also include all members of management one level below the executive directors including all functional heads.

(G) Shareholders

- (i) In case of the appointment of a new director or re-appointment of a director the shareholders must be provided with the following information:
 - (a) A brief resume of the director;
 - (b) Nature of his expertise in specific functional areas;
 - (c) Names of companies in which the person also holds the directorship and the membership of Committees of the Board; and
 - (d) Shareholding of non-executive directors as stated in Clause 49 (IV) (E) (v) above
- (ii) Quarterly results and presentations made by the company to analysts shall be put on company's web-site, or shall be sent in such a form so as to enable the stock exchange on which the company is listed to put it on its own web-site.

- (iii) A board committee under the chairmanship of a non-executive director shall be formed to specifically look into the redressal of shareholder and investors complaints like transfer of shares, non-receipt of balance sheet, non-receipt of declared dividends etc. This Committee shall be designated as 'Shareholders/Investors Grievance Committee'.
- (iv) To expedite the process of share transfers, the Board of the company shall delegate the power of share transfer to an officer or a committee or to the registrar and share transfer agents. The delegated authority shall attend to share transfer formalities at least once in a fortnight.

V. CEO/CFO Certification

The CEO, i.e. the Managing Director or Manager appointed in terms of the Companies Act, 1956 and the CFO i.e. the whole-time Finance Director or any other person heading the finance function discharging that function shall certify to the Board that:

- (a) They have reviewed financial statements and the cash flow statement for the year and that to the best of their knowledge and belief :
 - (i) these statements do not contain any materially untrue statement or omit any material fact or contain statements that might be misleading;
 - (ii) these statements together present a true and fair view of the company's affairs and are in compliance with existing accounting standards, applicable laws and regulations.
- (b) There are, to the best of their knowledge and belief, no transactions entered into by the company during the year which are fraudulent, illegal or violative of the company's code of conduct.

Training Material on Internal Audit

- (c) They accept responsibility for establishing and maintaining internal controls and that they have evaluated the effectiveness of the internal control systems of the company and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies.
- (d) They have indicated to the auditors and the Audit committee:
 - (i) significant changes in internal control during the year;
 - (ii) significant changes in accounting policies during the year and that the same have been disclosed in the notes to the financial statements; and
 - (iii) instances of significant fraud of which they have become aware and the involvement therein, if any, of the management or an employee having a significant role in the company's internal control system

VI. Report on Corporate Governance

- (i) There shall be a separate section on Corporate Governance in the Annual Reports of company , with a detailed compliance report on Corporate Governance. Non-compliance of any mandatory requirement of this clause with reasons thereof and the extent to which the non-mandatory requirements have been adopted should be specifically highlighted. The suggested list of items to be included in this report is given in **Annexure- I C** and list of non-mandatory requirements is given in **Annexure – I D**.
- (ii) The companies shall submit a quarterly compliance report to the stock exchanges within 15 days from the close of quarter as per the format given in **Annexure I B**. The report

shall be signed either by the Compliance Officer or the Chief Executive Officer of the company.

VII. Compliance

- (1) The company shall obtain a certificate from either the auditors or practicing company secretaries regarding compliance of conditions of corporate governance as stipulated in this clause and annex the certificate with the directors' report, which is sent annually to all the shareholders of the company. The same certificate shall also be sent to the Stock Exchanges along with the annual report filed by the company.
- (2) The non-mandatory requirements given in **Annexure – I D** may be implemented as per the discretion of the company. However, the disclosures of the compliance with mandatory requirements and adoption (and compliance) / non-adoption of the non-mandatory requirements shall be made in the section on corporate governance of the Annual Report.

ANNEXURE I A

Information to be placed before Board of Directors

1. Annual operating plans and budgets and any updates.
2. Capital budgets and any updates.
3. Quarterly results for the company and its operating divisions or business segments.
4. Minutes of meetings of audit committee and other committees of the board.
5. The information on recruitment and remuneration of senior officers just below the board level, including appointment or removal of Chief Financial Officer and the Company Secretary.
6. Show cause, demand, prosecution notices and penalty notices which are materially important.
7. Fatal or serious accidents, dangerous occurrences, any material effluent or pollution problems.
8. Any material default in financial obligations to and by the company, or substantial non- payment for goods sold by the company.
9. Any issue, which involves possible public or product liability claims of substantial nature, including any judgement or order which, may have passed strictures on the conduct of the company or taken an adverse view regarding another enterprise that can have negative implications on the company.
10. Details of any joint venture or collaboration agreement.
11. Transactions that involve substantial payment towards goodwill, brand equity, or intellectual property.

Clause 49 – Corporate Governance

12. Significant labour problems and their proposed solutions. Any significant development in Human Resources/ Industrial Relations front like signing of wage agreement, implementation of Voluntary retirement Scheme etc.
13. Sale of material nature, of investments, subsidiaries, assets, which is not in normal course of business.
14. Quarterly details of foreign exchange exposures and the steps taken by management to limit the risks of adverse exchange rate movement, if material.
15. Non-compliance of any regulatory, statutory or listing requirements and shareholders service such as non-payment of dividend, delay in share transfer etc.

ANNEXURE I B

Format of Quarterly Compliance Report on Corporate Governance

Name of the Company:

Quarter ending on:

Particulars	Clause of Listing agreement	Compliance Status Yes/No	Remarks
I. Board of Directors	49(I)		
(A) Composition of Board	49(IA)		
(B) Non-executive Directors' disclosures	49 (IB)		
(C) Other provisions as to Board and Committees	49 (IC)		
(D) Code of Conduct	49 (ID)		
II. Audit Committee	49 (II)		
(A) Qualified and Independent Audit Committee	49 (IIA)		
(B) Meeting of Audit Committee	49 (IIB)		
(C) Powers of Audit Committee	49 (IIC)		
(D) Role of Audit Committee	49 II(D)		
(E) Review of Information by Audit Committee	49 (IIE)		
III. Subsidiary Companies	49 (III)		
IV. Disclosures	49 (IV)		
(A) Basis of related party transactions	49 (IV A)		

Clause 49 – Corporate Governance

Particulars	Clause of Listing agreement	Compliance Status Yes/No	Remarks
(B) Board Disclosures	49 (IV B)		
(C) Proceeds from public issues, rights issues , preferential issues etc.	49 (IV C)		
(D) Remuneration of Directors	49 (IV D)		
(E) Management	49 (IV E)		
(F) Shareholders	49 (IV F)		
V. CEO/CFO Certification	49 (V)		
VI. Report on Corporate Governance	49 (VI)		
VII. Compliance	49 (VII)		

Note:

- 1) The details under each head shall be provided to incorporate all the information required as per the provisions of the Clause 49 of the Listing Agreement.
- 2) In the column No.3, compliance or non-compliance may be indicated by Yes/No/N.A.. For example, if the Board has been composed in accordance with the Clause 49 I of the Listing Agreement, "Yes" may be indicated. Similarly, in case the company has no related party transactions, the words "N.A." may be indicated against 49 (IV A).
- 3) In the remarks column, reasons for non-compliance may be indicated, for example, in case of requirement related to circulation of information to the shareholders, which would be done only in the AGM/EGM, it might be indicated in the "Remarks" column as – "will be complied with at the AGM". Similarly, in respect of matters which can be complied with only where the situation arises, for example, "Report on Corporate Governance" is to be a part of Annual Report only, the words "will be complied in the next Annual Report" may be indicated.

ANNEXURE I C

Suggested List of Items to Be Included In the Report on Corporate Governance in the Annual Report of Companies

1. A brief statement on company's philosophy on code of governance.
2. Board of Directors:
 - i. Composition and category of directors, for example, promoter, executive, non- executive, independent non-executive, nominee director, which institution represented as lender or as equity investor.
 - ii. Attendance of each director at the Board meetings and the last AGM.
 - iii. Number of other Boards or Board Committees in which he/she is a member or Chairperson
 - iv. Number of Board meetings held, dates on which held.
3. Audit Committee :
 - i. Brief description of terms of reference.
 - ii. Composition, name of members and Chairperson.
 - iii. Meetings and attendance during the year
4. Remuneration Committee:
 - i. Brief description of terms of reference.
 - ii. Composition, name of members and Chairperson
 - iii. Attendance during the year.
 - iv. Remuneration policy.

- v. Details of remuneration to all the directors, as per format in main report.
5. Shareholders Committee:
- i. Name of non-executive director heading the committee.
 - ii. Name and designation of compliance officer.
 - iii. Number of shareholders' complaints received so far.
 - iv. Number not solved to the satisfaction of shareholders.
 - v. Number of pending complaints.
6. General Body meetings:
- i. Location and time, where last three AGMs held.
 - ii. Whether any special resolutions passed in the previous 3 AGMs.
 - iii. Whether any special resolution passed last year through postal ballot – details of voting pattern.
 - iv. Person who conducted the postal ballot exercise.
 - v. Whether any special resolution is proposed to be conducted through postal ballot.
 - vi. Procedure for postal ballot.
7. Disclosures:
- i. Disclosures on materially significant related party transactions that may have potential conflict with the interests of company at large.
 - ii. Details of non-compliance by the company, penalties, strictures imposed on the company by Stock Exchange or SEBI or any statutory authority, on any matter related to capital markets, during the last three years.
 - iii. Whistle Blower policy and affirmation that no personnel has been denied access to the audit committee.

- iv. Details of compliance with mandatory requirements and adoption of the non-mandatory requirements of this clause.
- 8. Means of communication.
 - i. Quarterly results.
 - ii. Newspapers wherein results normally published
 - iii. Any website, where displayed.
 - iv. Whether it also displays official news releases; and
 - v. The presentations made to institutional investors or to the analysts.
- 9. General Shareholder information:
 - i. AGM : Date, time and venue.
 - ii. Financial year.
 - iii. Date of Book closure.
 - iv. Dividend Payment Date.
 - v. Listing on Stock Exchanges
 - vi. Stock Code.
 - vii. Market Price Data : High., Low during each month in last financial year.
 - viii. Performance in comparison to broad -based indices such as BSE Sensex, CRISIL index etc.
 - ix. Registrar and Transfer Agents
 - x. Share Transfer System.
 - xi. Distribution of shareholding.
 - xii. Dematerialization of shares and liquidity.
 - xiii. Outstanding GDRs/ADRs/Warrants or any Convertible instruments, conversion date and likely impact on equity.
 - xiv. Plant Locations.
 - xv. Address for correspondence.

ANNEXURE I D

Non-Mandatory Requirements

(1) The Board

A non-executive Chairman may be entitled to maintain a Chairman's office at the company's expense and also allowed reimbursement of expenses incurred in performance of his duties.

Independent Directors may have a tenure not exceeding, in the aggregate, a period of nine years, on the Board of a company.

(2) Remuneration Committee

- i. The board may set up a remuneration committee to determine on their behalf and on behalf of the shareholders with agreed terms of reference, the company's policy on specific remuneration packages for executive directors including pension rights and any compensation payment.
- ii. To avoid conflicts of interest, the remuneration committee, which would determine the remuneration packages of the executive directors may comprise of at least three directors, all of whom should be non-executive directors, the Chairman of committee being an independent director.
- iii. All the members of the remuneration committee could be present at the meeting.
- iv. The Chairman of the remuneration committee could be present at the Annual General Meeting, to answer the shareholder queries. However, it would be up to the Chairman to decide who should answer the queries.

(3) Shareholder Rights

A half-yearly declaration of financial performance including summary of the significant events in last six-months, may be sent to each household of shareholders.

(4) Audit Qualifications

Company may move towards a regime of unqualified financial statements.

(5) Training of Board Members

A company may train its Board members in the business model of the company as well as the risk profile of the business parameters of the company, their responsibilities as directors, and the best ways to discharge them.

(6) Mechanism for Evaluating Non-executive Board Members

The performance evaluation of non-executive directors could be done by a peer group comprising the entire Board of Directors, excluding the director being evaluated; and Peer Group evaluation could be the mechanism to determine whether to extend / continue the terms of appointment of non-executive directors.

(7) Whistle Blower Policy

The company may establish a mechanism for employees to report to the management concerns about unethical behaviour, actual or suspected fraud or violation of the company's code of conduct or ethics policy. This mechanism could also provide for adequate safeguards against victimization of employees who avail of the mechanism and also provide for direct access to the Chairman of the Audit committee in exceptional cases. Once established, the existence of the mechanism may be appropriately communicated within the organization.