Guide on

Risk-based Internal Audit

Committee on Internal Audit

The Institute of Chartered Accountants of India

(Set up under an Act of Parliament)

O 3 442 21

Guide on Risk-based Internal Audit

Committee on Internal Audit

The Institute of Chartered Accountants of India

(Set up under an Act of Parliament)

First Edition: November 2007

Price: Rs. 250

ISBN No. 978-81-8441-008-2

E-mail: cia@icai.org
Website: http://www.icai.org

Published by
Vijay Kapur, Director
The Institute of Chartered Accountants of India
'ICAI Bhawan', Indraprastha Marg
New Delhi - 110 002 INDIA

Cover & Illustrations
Narendra Bhola

Realisation
Sterling Preferred Printing
New Delhi INDIA

Guide on Risk-based Internal Audit

The Institute of Chartered Accountants of India

(Set up under an Act of Parliament)

The basic draft of this Guide was prepared by the study group under the convenorship of CA. Deepak Wadhawan, its members being CA. R.N. Joshi, CA. Neville Dumasia, CA. Pankaj Sahai, CA. Srikant Sarpotdar and CA. Swapnil Kabra.

The views expressed in the Guide are those of the authors and may not necessarily be the views of their employers.

Contents

Contents

Foreword

Foreword

With a dynamic entrepreneurial environment, which is changing and probably becoming more difficult to cope with every passing day, and the steeply rising expectations of the stakeholders in these entrepreneurial ventures, keeping pace and more often than not surpassing the changes in the entrepreneurial environment has everybody involved in running that venture on their toes. In that scenario, chartered accountants have a critical role to play whether at the forefront or at the back office.

But to be able to play an instrumental role in the sustained growth and meaningful development of a business, an Industry, the economy and the society, it is essential that we keep our knowledge base and skill sets at their sharpest best. The biggest challenge today, however, is not just keeping abreast with the existing technical knowledge and skills, but to imbibe such as are able to help us pre-empt the changes in the business environment and the stakeholders' expectations and adapt to the same. Whereas, the Institute is committed to that concern, and brings out a number of technical publications, organizes various dedicated conferences, seminars, workshops. At this juncture, I would also urge the members to come forward and

actively participate in development of the technical literature and share their invaluable treasure of knowledge and experience with their professional colleagues.

In addition to the above, it is equally essential that the members also remain alert to relevant developments at the global front. That, with the spread and penetration of technology to even the most interior parts of the country, I feel, should not be a difficult task, what is necessary is the commitment and zeal in our hearts.

Only when we are able to embed that commitment and zeal in our hearts, would we be *partners in national building* in real sense of the word.

New Delhi
2nd November, 2007

CA. SUNIL H. TALATI
President, ICAI

Preface

Preface

Traditionally, the main focus of the internal audit was confined to the controls and processes relating to financial transactions. Even in certain entities, internal audit was more used as review and inspection. With the passage of time and combined with the growth of organisations, the managements view internal audit as a significant resource in evaluating entire operations and achieve more effectiveness in day to day activities. In today's era of globalisation, the emergence of new models of governing the enterprises, a subtle shift towards controls and strategic decisionmaking, identification and assessment of risk has become one focal point. In recent times, the risk-based internal audit is being viewed by the management as an important tool to assess the management of the risks that are barriers to the objectives and success of the organization. Risk-based internal audit involves the assessment of the risks' maturity level, expressing opinion on adequacy of the policies and processes established by the management to manage the risks. Risk-based internal audit mainly report on the risk management that includes identification, evaluation, control and monitoring of the risk. A risk-based internal audit mainly focuses on the objectives rather than looking at the controls and transactions. This demands the internal auditor to have the skills to provide broad level of the assurance to the management.

Keeping this in mind, the Committee on Internal Audit is issuing this Guide on Risk-based Internal Audit as a part of series of the publications on Internal Audit. This guide would help the members of the Institute as well as others to understand not only the concept of the risk-based internal audit but also the methodology of the same.

This Guide is divided into six chapters with a view to provide the guidance regarding the risk-based internal audit to all the readers. Chapter 1, Introduction, would help the readers to understand the concept of the risk-based internal audit. Chapter 2, Risk Management, deals with aspects such as understanding risk, basic concepts of risk management, enterprise wide risk management, risk maturity of an organisation. Chapter 3, Using Risk-based Internal Audit Methodology, covers the building blocks of RBIA, stages in RBIA and a case study. Chapter 4, The Internal Audit Process explains the phases of the internal audit process. Chapter 5, Some Pitfalls and The Way Ahead describes the prospective picture of the RBIA. The Guide also contains the Exhibits and Appendices illustrating complex subjects in a simplified manner for easy understanding of the readers.

I am grateful to CA. Deepak Wadhawan, convenor of the study group and its members, CA. R. N. Joshi, CA. Neville Dumasia, CA. Pankaj Sahai, CA. Shrikant Sarpotdar and CA. Swapnil Kabra for squeezing the time to prepare the draft of the Guide.

I am also thankful to CA. Sunil H. Talati, President, ICAI and CA. Ved Kumar Jain, Vice President, ICAI for their continuous support. I also wish to thank all the members of the Committee, CA. Charanjot Singh Nanda, (Vice Chairman), CA. Rajkumar S. Adukia, CA. Atul Chunilal Bheda, CA. Sanjeev Krishnagopal Maheshwari, CA. Mahesh Pansukhlal Sarda, CA. Shanti Lal Daga, CA. J. Venkateswarlu, CA. Anuj Goyal, CA. Amarjit Chopra, Shri Manoj K. Sarkar, CA. Prashant S. Akkalkotkar, CA. Shyam Lal Agarwal, CA. Vivek R. Joshi, CA. Krishan Lal Bansal, CA. Satyavati Berera, CA. Brij Bhushan Gupta, CA. Anil Jain for their valuable support.

I am sure that this Guide would help the readers in learning techniques and methodologies that would boost their skills to divert the audit process to risk based approach.

Kolkata
5th November, 2007

CA. ABHIJIT BANDYOPADHYAY
Chairman
Committee on Internal Audit

1 Introduction

One

Background

1.1. During recent years, managements are increasingly getting risk focused. Expectations from internal auditors are hence shifting from providing an assurance on the adequacy and effectiveness of internal controls to an assurance on whether risks are being managed within acceptable limits as laid down by the Board of Directors. This shift in assurance from a control based focus to a risk based focus requires that the internal audit activity be carried out by an experienced multidisciplinary team using risk-based internal audit (RBIA) methodology.

1.2. The objective of this Guide is to provide guidance to the members of the Institute, as to the concepts and steps involved in risk-based internal audit (RBIA) methodology.

Internal Audit - Definition, Objectives and Scope

1.3. Preface to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India defines the term "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."

1.4. To achieve the objectives of appraising and suggesting improvements in the overall governance mechanism of the organisation, internal auditors have been carrying out assurance and consulting activities in the following areas:

a. Internal policy compliance.

b. Regulatory policy compliance.

c. Process improvement.

d. Training and development.

Assurance and consulting activities undertaken by internal auditors in the above four areas have normally taken the shape of the following activities:

- Examination and evaluation of the adequacy and effectiveness of the internal control system.
- Undertaking risk assessments in focus areas, either as a consulting activity or as an input to the internal audit plan.
- Review of financial information system, Management Information System (MIS) and the underlying technology platform that delivers this electronic data.
- Review of the accuracy and reliability of accounting records and financial reports.
- Review of safeguarding of assets.
- Appraisal of the economy and efficiency of activities in operational areas.
- Carrying out process improvement activities through business process audits.
- Carrying out performance reviews of functions through operational audits.
- Review of the systems established to ensure compliance with legal and regulatory requirements, code(s) of conduct and the implementation

review of policies and procedures.

- Testing the reliability and timeliness of legal compliance.
- Using the internal audit department as a training ground for developing finance and accounts managers.

Need for Internal Audit and the "Expectation Gap"

1.5. In spite of the above activities and the mission - critical area of corporate governance that it operates in, the internal audit function has been historically viewed as stable and beneficial but not necessarily essential for the organization. Internal audit has traditionally drawn its importance from the legal and regulatory framework in which the entity operates and it is likely that in some organizations it still owes its existence to it. Of late, many legislations across the world have reiterated the importance of sound and effective internal audit function as part of effective internal control framework (for example, the Sarbanes Oxley Act of 2002, London Stock Exchange Combined Code, backed up by the Turnbull Committee guidance, etc.) The Indian requirement is in Clause 49 of the listing agreement. Also The Companies Auditors Report Order 2003 provides for the statutory auditor to comment on internal audit function of listed companies and other companies having paid capital of more than Rs. 50 lakh or average annual turnover more than Rs. 5 crore for last 3 consecutive financial years thereby making Internal audit a tacit mandatory requirement in such companies.

1.6. The lower status of *"beneficial but not necessarily essential"* in the organization can only be attributable to an *"expectation gap"* between what the internal auditors are delivering as assurance/ consulting and what the management expects out of an essential function.

1.7. Management's focus is to meet the overall corporate objective and those in the business plan. The business environment is increasingly throwing up newer challenges and opportunities with globalization, disruptive technologies and rules being continuously rewritten. New risks are hence coming up frequently. Focus on internal controls does not give the organization an assurance on whether all the significant risks which can impact the objectives

of the organization are within acceptable levels as defined by the Board. Focus on risks and providing consulting and assurance services around a continuously updated *"risk register"* is probably the first step towards delivering to the management in accordance with their expectation and reducing the *"expectation gap"*.

Introduction to Risk-based Internal Audit

1.8. The objective of RBIA[1] is to provide independent assurance to the Board that:

- The risk management processes which management has put in place within the organisation (covering all risk management processes at corporate, divisional, business unit, business process level, etc.) are operating as intended.
- These risk management processes are of sound design.
- The responses which management has made to risks which they wish to treat are both adequate and effective in reducing those risks to a level acceptable to the Board.
- And a sound framework of controls is in place to sufficiently mitigate those risks which management wishes to treat.

1.9. Hence the internal audit report is on the management of significant risks of the organization and the assurance is on these risks being managed within the acceptable limits as laid down by the Board of Directors.

To give this assurance the internal auditor would carry out:

- *a process audit on risk management processes at all levels of the organization, viz., corporate, divisional, business unit, business process level, etc.,* put in place by line management so as to assess the adequacy of their design and compliance.
- *a transactional audit on the significant risks* so as to assess whether the risk response puts the risk within acceptable limits.

By doing so, the RBIA methodology links the internal audit activity to an organisation's overall risk management framework. At the risk register level, the link between management of risks and its audit is done by adding the audit procedure, and other relevant audit information against each risk. This

1 Position Statement on RBIA issued by the Institute of Internal Auditors - UK and Ireland

set of documents is known as the risk and audit universe (RAU). *(Refer to Exhibit 6).*

Comparison with Traditional Internal Audit

1.10. RBIA is not different from internal audit. It represents internal auditing using a risk-based methodology. Under the traditional internal audit approach, the internal auditors are required to confirm that the controls are operating effectively. Internal auditors then make recommendations where the controls are not effective. Although traditional internal audit concentrates on riskier areas of the organisation, its approach is based on its own assessment of risk. RBIA bases itself on the underlying fact that the organisation's management is responsible for risk management across the organisation. It audits the risk management processes built by the management and if found reliable bases its audit efforts around management's assessment of risk. RBIA hence ensures that the audit resources are utilised towards assessing the management of most significant risks. RBIA approach has greater involvement of organisation's management as many risks being dealt with are very significant to the organisation. RBIA may involve audit of new areas in the organisation that internal auditors had not covered before. RBIA does not necessarily change the auditing techniques to be used. However, the audit tests and techniques under RBIA focus on ensuring the effectiveness of controls which treat risks. Neither are the tests specially designed to detect incorrect and fraudulent transactions, nor does it deploy resources on insignificant risks.

1.11. Internal auditors while following the RBIA methodology may also notice the following subtle differences during the 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 organization, 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.

- For organizations at a lower risk maturity level, performing both consulting and assurance activities.
- Redundancy of structured audit programs as individual risks are listed in the audit plan.
- Heightened management participation during all phases of the audit.
- Management pressure for an experienced multidisciplinary team whose members are first business managers and then internal auditors.

Before discussing the process of RBIA in detail, it is important to understand 'risks' and 'risk management'.

Risk Management

2 Two

A. Understanding Risk

Meaning of Risk

2.1 Organisations exist for a purpose. Whereas the private sector strives to enhance shareholder value, the Government and Not for Profit organizations have a main purpose of delivering service or other benefits in public interest.

2.2 Achievement of organisational objectives is surrounded by uncertainties which both poses threats to and offers opportunity for increasing success. Changing circumstances, such as rising interest rates, can be an opportunity for an organization with surplus cash and a risk for a borrower. Hence these circumstances need to be seen with reference to the organisation's objective.

- When used in the broad sense, risks are those uncertainties of outcome, whether a opportunity or threat, arising out of actions and events.
- When defined narrowly, risks are those uncertainties which impede the achievement of the objective.

In this Guide, the term "risk" is used in the narrow sense.

Risk Attributes-Their Measurement and Risk Score

2.3 All risks have two attributes, *viz.*

- Likelihood of risk occurrence.
- Risk consequence.

2.4 To facilitate understanding and usability in decision making of risk, comparison helps. To enable comparison a risk score is used. By measuring the two risk attributes a risk score can be derived for that risk. This risk score is meant for comparison between a cut off point normally the *'risk appetite'* or comparing to other risks thereby filtering for *'significant risks'*.

2.5 The measurement of the likelihood of risk is normally against five levels on a scale of 5, *viz.*

- Remote (score 1).
- Unlikely (score 2).
- Possible (score 3).
- Likely (score 4).
- Almost certain (score 5).

Exhibit 1 contains details of the measurement yardstick for likelihood of risk.

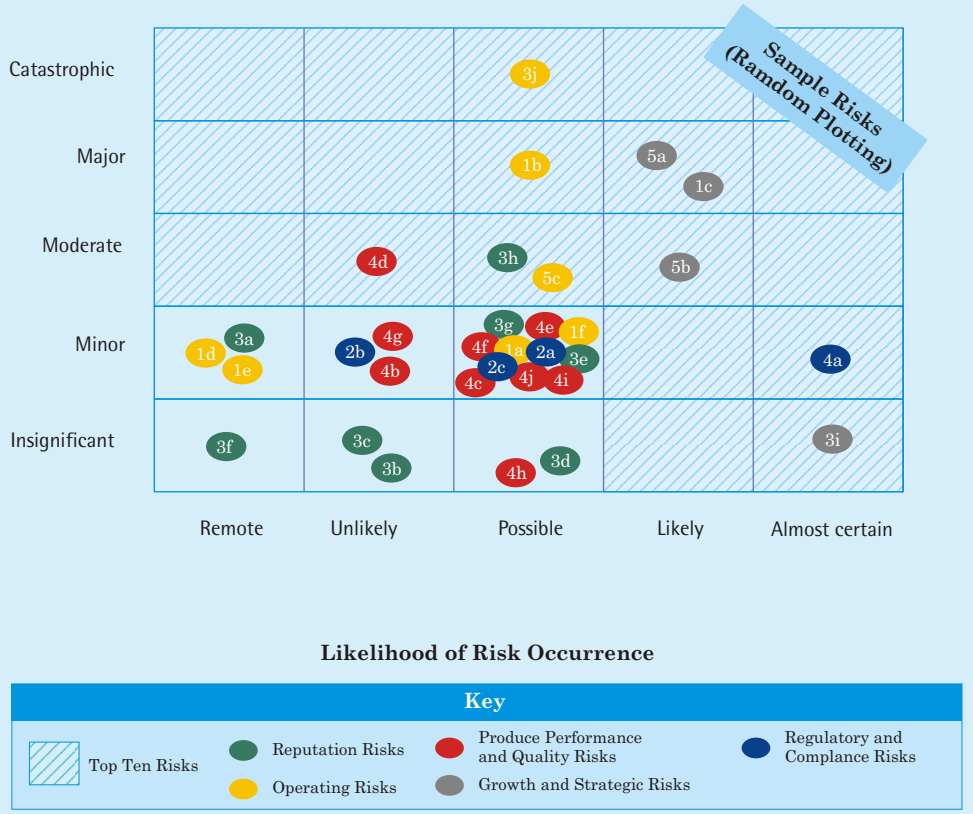
2.6 Risk consequences can also be against five levels on a scale of 5, *viz.*

- Insignificant (score 1).
- Minor (score 2).
- Moderate (score 3).
- Major (score 4).
- Catastrophic (score 5).

Appendix 1 contains details of the measurement yardstick for risk consequences. A risk with the lowest level of likelihood, i.e., remote (score 1) can nevertheless have the highest level of consequences, i.e., catastrophic (score 5). This can be explained by way of an example: The likelihood of floods causing damage to the distribution network of an electricity distribution company can be 'remote' but the consequences of damage can be 'catastrophic'. In such a scenario existence of a contingency plan becomes important.

2.7 Risk score for that risk is a numeric multiple of the likelihood of the risk and the risk consequences. As an example the Board may have a risk appetite of 12 and any risk with a score above 12 becomes significant risk and to be included in the audit plan. For a better understanding, risk score can be plotted on a chart as below which is known as a *"risk heat map"*.

Figure 1: Risk Heat Map



Business Risk

2.8 Business risks impede the achievement of the organisation's goals and objectives and have been explained in detail in this chapter.

Audit Risk

2.9 Audit risk relates mainly to the internal and external audit efforts to achieve its objectives, i.e., provide effective, timely and efficient assurance to the Board. Audit risk has traditionally been seen strictly as the risk of incorrect audit conclusions. Contemporary views however include big-picture audit risks; specifically, that the internal audit function is not doing the right things or working in the best ways.

2.10 Even from internal auditing perspective, an organization with well established risk management processes decreases audit risk. Where the organization has a formal enterprise-wide risk management program (ERM) in place, the internal auditor would assess it for design adequacy and compliance to decide whether to rely on the risk register and where found reliable then focus on auditing the risk responses to significant risks. By relying on significant risks as determined by management, internal auditing becomes more efficient.

Classification of Business Risk

2.11 Business risks are of a diverse nature. For example, risks can be classified as internal and external risks; controllable and uncontrollable risks, etc. These classifications help in risk identification and a better understanding of the interplay between the risks themselves and between objectives, strategies, processes, risks and controls during risk assessment.

Business Risks: Internal and External

2.12 Internal risks arise from events taking place within the business enterprise. Such risks arise during the ordinary course of a business. These risks can be forecasted and the probability of their occurrence can be determined. Hence, they can be controlled by management significantly. Internal factors giving rise to such risks include:

- *Human factors* as strikes and lock-outs by trade unions; negligence and dishonesty of an employee; accidents or deaths in the factory, etc.
- T*echnological factors* unforeseen changes in the techniques of production or distribution resulting into technological obsolescence, etc.

- *Physical factors* as fire in the factory, damages to goods in transit, etc.

2.13 External risks arise due to events occurring outside the business organisation. Such events are generally beyond the control of the management. Hence, determining the likelihood of the resulting risks cannot be done with accuracy.

External factors giving rise to such risks include:

- *Economic factors* as price fluctuations, changes in consumer preferences, inflation, etc.
- *Natural factors* as natural calamities such as earthquake, flood, cyclone, etc.
- *Political factors* as fall or change in the Government resulting into changes in government policies and regulations, communal violence or riots, hostilities with the neighboring countries, etc.

Business Risks: Controllable and Non-controllable

2.14 Controllable risks arise from the events taking place within the business enterprise. Such risks arise during the ordinary course of business. These risks can be forecasted and the probability of their occurrence can be determined. Hence, they can be controlled by management to an appreciable extent (e.g., risks of fire, storms, etc.). Controllable risks need not necessarily be prevented, but the financial loss can be minimised (e.g., insurance cover can be purchased to recover the financial loss due to fire).

2.15 Uncontrollable risks however, are those that would have a detrimental financial impact but cannot be controlled. Some uncontrollable risks that are common to many businesses include:

- Recessionary economy.
- New competitor locating nearby.
- New technology.

Each business faces risks that are unique to that business. Businesses should consider these carefully and briefly describe what steps would be taken if an uncontrollable risk actually happens to the business (contingency plan). For example, if the risk of a recession would severely affect the company,

management may consider what products or services could be offered that would not be as sensitive to a recessionary economy.

Risk Categories by COSO

2.16 The COSO framework categories risks as Operations, Financial Reporting, and Compliance. This categorization is illustrated below:

- *Efficiency and effectiveness of operations*-e.g., the company does not meet strategic objectives, the process does not operate efficiently, customers are not satisfied with services received, etc.
- *Financial Reporting*-e.g., the absence of a key financial control causes a material error in the financial statements.
- *Compliance with laws and regulations*-e.g., the company is in violation of applicable regulatory requirements.

B. Basic Concepts of Risk Management

Risk Capacity

2.17 Risk capacity shows how much risk the organization can absorb.

Risk Appetite

2.18 Risk appetite shows how much risk the management is willing to accept.

Risk Response

2.19 The purpose of assessing and addressing risks is to constrain them to a tolerable level within the risk appetite of the organization. Response to risks can be of the following types:

Tolerate:

The exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained.

In these cases, the response may be to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning for handling the impact that will arise if the risk is realized.

Transfer:

For some risks the best response may be to transfer them. This might be done by conventional insurance or by paying a third party to take the risk.

This option is particularly good for mitigating financial risks or risks to assets. The transfer of risks may be considered to either reduce the exposure of the organization or because some other organization is more capable of effectively managing the risk.

It is important to note that some risks are not (fully) transferable in particular, it is generally not possible to transfer reputation risk even if the delivery of a service is contracted out.

Terminate:

Some risks can only be treatable, or containable to acceptable levels, by terminating the activity itself. This option can be particularly important in project management if it becomes clear that the projected cost-benefit relationship is in jeopardy as the cost of treating the risk does not make the activity viable. For example, land acquisition for a project whose feasibility is based on that particular land may be risky and the cost of treating it in terms of legal fees is so high, that it may be better to terminate the project.

Treat:

By far, a large number of risks will be addressed in this way. The purpose of treatment is that whilst continuing with the activity giving rise to the risk, action (internal control) is taken to constrain the risk to an acceptable level.

Inherent Risk and Residual Risk

2.20 Inherent risk is the level of risk assuming no internal controls, while residual risk is the level of risk after considering the impact of internal controls. Example the risk of 'over/ understatement of revenue' without considering any internal controls indicates inherent risk. The above risk when considered with internal controls in place (say, monthly reconciliation of revenue and follow up, correction of discrepancies, etc.) indicate residual risk.

2.21 The objective of internal controls is to reduce the inherent risk and keep the residual risk within the organization's risk appetite. The gap between the inherent risk and residual risk shows the strength of the control and is known as the control score.

Entity Risk Assessment and Business Process Risk Assessment

2.22 Entity risk is the assessment of strategic risks. Organizational objectives and strategies are delivered through business processes; hence business process risk assessment is the preferred way to carry out the exercise.

Significant Risk

2.23 Significant risk is a term used by internal auditors where in their assessment the risk is significant enough to include it in the audit plan. Usually these risks in their inherent state have a risk score higher than the risk appetite for that risk.

Risk Register

2.24 Risk register is a record of risk, risk assessments; risk mitigation and action plans prepared by the responsible parties that help support the overall ERM and controls disclosures reporting process.

2.25 Risk register is continuously updated and has columns for risk, causes, consequences, ownership, inherent risk score, controls, residual risk score, process, action for further mitigation, action owner, due date, etc.

C. ERM - Enterprise Wide Risk Management

ERM and Risk Appetite of the Board

2.26 Enterprise Risk Management (ERM) is defined as a process, affected by an entity's board of directors, management, and other personal, 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.[2]

2.27 ERM includes the following activities:

- Determining the risk appetite.
- Establishing an appropriate internal environment, including a risk management policy and framework.
- Identifying potential threats to the achievement of its objectives and assessing the risk, i.e., the impact and likelihood of the threat occurring.
- Undertaking control and other response activities.
- Communicating information on risks in a consistent manner at all levels in the organization.
- Centrally monitoring and coordinating the risk management processes and the outcomes, and
- Providing assurance on the effectiveness with which risks are managed.

2.28 The term *'risk appetite'* used in the above definition refers to the extent of risk that the Board is willing to take to pursue the objectives. Risk appetite setting is done at different levels, *viz.* for the organization at the entity level, process level, and different risk groups and for individual key risks. Risk appetite provides a standard against which a risk can be compared and where the risk is above the risk appetite, it is considered a threat to the reasonable assurance that the objective will be achieved.

2.29 While risk appetite is to be set lower than the risk capacity; however, with an aggressive Board, the risk appetite can be higher than the risk capacity. For example, the Board may decide on utilizing the cash flow for operational purposes in the short term for earmarked funds meant for payment of quarterly installment of taxes. This could result in default of payment on due date and hence becomes a significant risk which needs to be covered by the internal auditor and reported upon even though the risk may be within the risk appetite. However, in the normal course, internal auditors are expected to

2 Defined by COSO (Committee of Sponsoring Organisations of Treadway Commission)

take the risk appetite as a given and evaluating the risk appetite is out of audit scope. Internal auditors can, however, do a consulting activity of assisting the Board in fixing the risk appetite and its documentation.

2.30 ERM is a new approach in the ways organizations are assessing, managing and communicating business risks. By assisting organizations climb up on the risk maturity scale, ERM makes a major contribution towards helping an organization manage risks to achieve its objectives. ERM helps an organization become a risk managed business. A fundamental question that emerges is how should the internal audit effectively audit the risk management processes that are being developed. Risk Based internal audit methodology provides an answer by providing assurance to the management and the Board on the effectiveness of risk management processes.

ERM as a part of Clause 49 Compliance

2.31 As per Clause 49 of the listing agreement, Board disclosures are to be made on whether the following is being carried out on 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 a proper defined framework".

2.32 To implement the requirements of the above clause, organizations tend to introduce certain risk management processes and identify strategic risks mainly to fulfill compliance requirements. Over a period of time as management begin realizing the advantages of assessing risks through an enterprise wide structured, consistent and continuous process, it normally introduces ERM in a full fledged way as a strategic management tool.

2.33 An ERM policy is first put in place which defines the guiding principles showing responsibility of line management for ERM and the broad activities covered by the risk management processes. A risk management framework to implement the ERM policy is then finalized showing the activities which need to be carried out and how they are to be carried out under three processes, *viz.*

- Risk assessment.
- Risk management.
- Risk communication.

Implementation is facilitated by a risk manager or the internal auditor as a consulting assignment. Subsequently risk based internal audit is carried out.

D. Risk Maturity of an Organization

Importance of Risk Maturity

2.34 RBIA provides an assurance on the effectiveness of risk management processes. The specific approach to be adopted during internal audit using RBIA methodology depends upon the internal auditor's assessment of the organisation's risk maturity. Risk maturity has levels which reflect the extent to which an organization understands its risks and has implemented ERM.

2.35 Some organizations especially those in a fast growth mode have an organizational culture which promotes operational mangers to remain at the risk naïve/ risk aware level. This means that the line managers are not expected to identify risks and if they do, it is confined to their personal knowledge or within their functional team. The internal control environment may be well defined but again it is to be operated by the staff management (such as the accounts manager), the logic being that line managers need to spend maximum time in operations and not be defocused by unnecessary paper work or issues other than their operations. In this mindset, coordinating activities and problem solving is considered as operations while risk assessment and management is considered a staff function. This model works well in a supply side market wherein the organization sells whatever it produces but flounders in a competitive and dynamic market wherein new risks arise periodically and the staff management who are not market facing are not fast enough to incorporate new controls to address these risks.

2.36 A risk naïve/risk aware organization in today's dynamic environment exhibits

inefficiencies as a continuous long list of pending issues at all times with the line manager or even mundane issues as goods received but unreconciled with Purchase Orders, delayed supplier payments resulting in line managers chasing accounts department for release of payment, etc., wherein the root cause is usually a risk which has not been addressed. In a risk aware organization, the silo approach culture wherein the manager tracks and addresses new risks related to his department only rather than in the business process usually throws up big losses arising out of customer dissatisfaction or failure of an enterprise wide activity such as implementing ERP.

2.37 The audit strategy depends upon the organization's risk maturity. Organizations at low risk maturity levels may require internal auditors to consult by promoting and advising on identification of and response to risks. For organisations with high risk maturity, the internal auditor would need to concentrate more on carrying out process audits of the risk management processes and especially reviewing the risk assessment process wherein the inherent risk (untreated) are identified, estimated (scored) and evaluated (compared with risk appetite).

Risk Maturity Levels

2.38 The following aspects in the organisation indicate its risk maturity. Internal auditors should refer to the same for concluding on the organisation's risk maturity:

- Business objectives are defined and communicated.
- Risk appetite is defined and communicated across the organisation.
- Control environment is strong. Including the tone from the top.
- Adequate processes exist for the assessment, management and communication of risks.

A suggested score card to assess risk maturity is given in Appendix 2.

2.39 To determine the level of risk maturity the internal auditors need to undertake the following activities:

- Meet the senior management to understand the organisation's risk management policy and risk framework along with management's

assessment on the level of implementation.

- Assemble the available information and documentation such as
- Organization's objectives:
  - Processes for risk assessment (identification, estimation and evaluation).
  - Definition of risk appetite.
  - Process of risk management, *viz.*, consideration of risks and associated controls in decision making process (example, in project evaluation).
  - Process of communication on the working of risk management through monitoring controls, MIS reports, etc.
  - Documentation on risks as risk register.
- Interview and discuss with managers as to their understanding of the risk management processes and their response to risks in their operations.

2.40 The table given below shows the levels of risk maturity.

Table 1: Key Characteristics at Different Levels of Risk Maturity

Risk Maturity	Key Characteristics
Risk Naive	No formal approach developed for risk management.
Risk Aware	Scattered silo based approach to risk management. Risks identified within functions and not across processes. Also risks not communicated across enterprise.
Risk Defined	Strategy and policy in place and communicated. Risk appetite defined.
Risk Managed	Enterprise wide approach to risk management developed and communicated. Risk register in place.
Risk Enabled	Risk management and internal control fully embedded into operations. Organization in readiness to convert market uncertainties into opportunities.

2.41 The internal audit approach is determined by the level of risk maturity identified above.

A. Risk Aware and Risk Naive

No risk register will be available in this type of organisation. As a consulting assignment, internal audit may be asked (in conjunction with management) to determine the work required to implement a risk framework which fulfils the requirements of the Board.

In such an organization, the focus of internal audit is necessarily on the controls. As same extent of risk assessment is in progress, some information on risks is available. The level of assurance on the controls would be higher if the internal auditor uses the key risks agreed with management to formulate the audit plan. The audit approach in this case would revolve around:

- Using the available information on risks during the planning stage for individual audits (discussed further in Chapter 4).
- Where management does not understand risks, conducting management training and risk facilitation workshops.

Despite a mention of the term "risks", the internal audit, as mentioned earlier, would provide assurance only on controls and not on the management of risks. Accordingly, the audit methodology is a modification of the traditional audit process and not RBIA. Also, care should be taken that as internal auditors are not primarily responsible for risk management, they should not determine risks without management involvement.

B. Risk Defined

In this type of organization, the understanding of risk management is patchy and the list of risks may not have been compiled into a complete risk register. As a consulting activity, internal audit in this case, would facilitate the compilation of a complete risk register from the list of risks already compiled by the managers. In areas where risk management is well defined, the internal auditor may use RBIA.

C. Risk Enabled and Risk Managed

This type of organisation represents a high level of understanding on the management of risk. A complete list of risks (risk register) is available for audit planning and the internal audit work would emphasize on whether risk management processes are working properly, responses to key risks and on the monitoring of controls.

3 Three

Using the Risk-based Internal Audit (RBIA) Methodology

A. Building Blocks of RBIA

Future Direction of Internal Auditing

3.1 As its primary activity, internal auditing is heading towards promoting risk management in an organization, periodically assessing risk maturity and for reasonably risk matured organizations (thereby auditable under RBIA methodology), giving an assurance on the adequacy and effectiveness in managing risks that threaten the achievement of the defined objectives. The measuring yardstick for managing risks is the risk appetite as laid down by the Board.

Audit is of Management of Risk and not of Risk

3.2 *Management estimates of inherent risks are out of scope*: The internal auditor should comment on whether the process laid down for risk assessment (risk identification, estimation and evaluation) is adequate and has been followed. A competent management will, however, not encourage the internal auditor to give assurance on management estimates, example whether risks have been correctly identified, whether inherent risk scores are accurate, etc. Usually the more strategic the risk, lesser would be the tolerance to the internal

auditor's opinions on risk management estimates. On the other hand, there are everyday examples of catastrophic risks. Also, there could be error indicators, example, in a known flood prone area the risk on account of flooding has not been taken in the risk register.

It may happen that the laid down risk processes were followed but there were errors in risk related management estimates. In such situations, the internal auditor should as a general practice, accept the management's inherent risk score as a given. Only where there are error indicators on risks, the audit report should bring out these error indicators and based on the likely severity of impact on the organization, follow up with a letter to the Audit Committee.

3.3 *Control score is auditable*: The difference between the two scores of a particular risk (*viz.*, inherent score and residual score) is the score of the risk response *viz.*, control score. An internal auditor being a domain expert on controls is expected to review the control score and comment whether in his assessment the residual risk score is higher from management's estimate, especially where the residual risk score exceeds the risk appetite.

3.4 *Risk maturity level is the reference point*: As explained earlier, the risk maturity level reflects the organization's understanding of its risks and the extent to which formal enterprise wide risk management is in place. The risk maturity level, hence, reflects the risk management environment and the tone on risks in the organization. It is, therefore, a reference point for the internal auditor to base his activities.

Key Reporting Areas on Management of Risks

3.5 Following from the above, it can be deduced that the internal audit reports should include the following:

- Assessment of the risk maturity levels, both at the organizational 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 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.

Assurance Requirements of the Board and Risk Appetite Should Always be Documented

3.6 The Board, through the Audit committee, may convey assurance requirements of HIGH, MEDIUM, and LOW for different areas. For example, non-compliance of certain labour laws can result in penal action against the directors. Hence, the assurance requirement will always be HIGH for such risk. Assurance requirements have a direct impact on the coverage, *viz.* audit plan, and hence needs to be documented and clearly understood.

3.7 Risk appetite can be different for the organization as a whole, for business units/ divisions, for a group of risks and for specific risks. Rarely Board puts a risk score for its risk appetite. However, without a quantified risk appetite, there is no benchmark to compare risks. In such a case, a consulting assignment to document the risk appetite may be the starting point.

Audit Strategy is Based on the Risk Maturity

3.8 Audit strategy under RBIA methodology has two elements, *viz.*

- Subject matter of the internal auditor's assurance
  - *Controls or risk management.*
- Nature of consulting services that the auditor plans to perform on risk management.
  - *Promoting, guiding and facilitating (PGF) or need based improvement* (NBI).

3.9 As there is both an assurance and consulting activity in the audit strategy, it implies that there is a threshold level of risk maturity in an organization, below which it is not possible to do an internal audit using RBIA methodology. For example, at the risk naïve and risk aware level, the internal auditor gives a traditional assurance on controls and provides consulting services in the

nature of promoting, guiding and facilitating (PGF) risk management. Based on the risk maturity the audit and consulting strategy (known commonly as the audit strategy) is determined. The audit strategy for different risk maturity levels[3] are as under:

Table 2 : Audit Strategy for Different Levels of Risk Maturity

Area	Risk Naive	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
Risk maturity report on enterprise wide risk management processes (RMP)	NO FORMAL RMP	POOR RMP	RMP DEFICIENCIES	RMP MANAGED ORGANISATION	RMP ENABLED ORGANISATION
Consulting objectives in risk management (RM)	To promote, guide, facilitate RM (PGF)	To promote, guide, facilitate RM (PGF)	To embed RM	To improve RM	Need based improvement (NBI)
Audit plan based on	Traditional audit plan (TAP)	Traditional audit plan (TAP)	Management view on risk (RBIA) and supplement with TAP	Management view on risk drives audit plan (RBIA)	Management view on risk drives audit plan (RBIA)
Assurance on	Control processes	Control processes	RMP and control processes	RMP	RMP

Selecting Individual Risks to Audit

3.10 The audit focus is to assess the control score of individual risks which have been selected. The internal auditor can adopt an inclusive approach to select the individual risks to be audited, *viz.*,

- Using the risk register, list the significant risks i.e., where the inherent score is above the risk appetite.
- Include risks where the management's assurance requirement is high.
- Include inherent risks appearing just within the risk appetite in key business processes, i.e., those processes that are associated with and

3 "An Approach to implementing Risk based Internal Auditing" issued by The Institute of Internal Auditors UK and Ireland.

manage a strategic risk of the organizational objectives.

- Include those inherent risks which are within the risk appetite but have a high score on one of the two parameters *viz.* likelihood or significance.
- Include risks with a large control score.
- Include risks based on information resulting from the organization's external audits and regulatory examinations.

Deciding the Frequency of Coverage

3.11 The frequency with which a risk would be covered in the internal audit depends upon aspects such as:

- Board's assurance requirement on that risk *viz.* high, medium, low.
- Whether one of the two risk components (likelihood/ consequences) of that individual risk is on an extreme (high/ low).
- Whether controls put the risk below the risk appetite.

Including the Risks into an Audit Assignment and the Importance of Selecting the Right *Auditable Unit*

3.12 As an auditing technique, risks are always analysed within a business process. Risks within a section of a business process are bunched logically into audit groups. For, example, risks in order booking of gold (See Exhibit 6C). Audit groups are then scheduled for internal audit. Audit groups are allocated to the internal auditor based on the latter's proficiency and availability.

3.13 In the case of a large business, an auditable unit can be different entity levels such as corporate office, division, business unit, a location, subsidiary, etc. The following situations may arise in such cases:

- Usually there are audit teams at different locations and hence a preference is given to location as an auditable unit.
- Usually business process as an auditable unit should be the logical choice not only because risks can be logically bunched into audit groups, but that business processes exist to fulfill organizational objectives and strategy, thereby the correct interpretation on the management of risks for strategic objectives can be arrived at. This may cut across locations and

could prove to be a challenge for the internal audit function. For, example, order fulfillment process for any product as cold rolled sheets or ribbed cotton fabric would involve looking at risks in processes as order booking, input inventory management, manufacturing management, finished goods inventory management and dispatches. In such cases, the internal auditor would give an assurance on the management of risks relating to fulfilling orders for that product. This assurance would be more valuable to management than separate internal audit reports on order booking, inventory, manufacturing, etc., which are not even product specific.

B. Stages in RBIA

3.14 Risk-based internal audit comprises of three stages, *viz.*,

- Assessing risk maturity.
- Preparing periodic audit plan.
- Conducting individual assurance audit assignments and reporting to appropriate levels.

Stage 1: Assessing risk maturity

The objective of assessing risk maturity is to decide which audit strategy to apply. Following steps are involved in this stage:

i. Understanding the risk maturity through discussions and documents.

ii. Concluding on the risk maturity.

iii. Submitting report to the audit committee on risk maturity; and

iv. Deciding on the audit strategy.

Stage 2: Preparing periodic audit plan

The objective of the periodic plan is to decide on which risk management processes (at different organizational entity levels) and which risk responses to audit and make a plan for carrying out individual audits. This stage normally involves the following:

i. Identifying risk responses and risk management processes on which objective assurance is required.

ii. Categorising and prioritising the risk.

iii. Linking risks to audit assignments.

iv. Preparing the periodic audit plan.

v. Allocating resources; and

vi. Completing the risk and audit universe.

Stage 3: Conducting Individual Assurance Audit Assignments and Reporting to Appropriate Levels

The objective of this stage is to execute the individual audit in a manner where the audit risk is least and to convey the findings on the risk responses and the risk management processes under audit to different levels of management. This stage comprises the following activities:

i. Assessing the assignment level risk maturity and reconfirming the assignment scope.

ii. Carrying out audit procedures on monitoring controls, control score of individual risks and compliance of laid down risk management processes by:

- discussing and observing monitoring of controls.
- collecting audit evidence through verification, walkthrough, Re-performance, etc., and, documenting the results of the audit work.

iii. Assessing management's evaluation of residual risks and concluding on responses and risk management processes covered by assignment and

iv. Reporting and feedback on action taken.

C. Case Study

ABC Bullion Trading Company

3.15 ABC Bullion Trading Company (ABC) has nation wide branches which sell gold to registered customers. ABC is consignment agents of a global bullion

company, and the Principal delivers gold directly to the branch. Prior to taking delivery, customers make advance payments of the full amount. Remittances made to the Principal are usually the day after the gold sale date and any loss/gain in foreign exchange is debited/ credited to the customer. There is a gold procedure manual whose workflow (sequence of activities) and internal controls are automated in a software application known as the Gold Management System (GMS). Head office has real time access to branch transactions as the GMS is online. Because of the high value of transactions and high inherent risk of physical loss, and the Board's assurance requirement being HIGH, the management wants the branch internal auditors to cover gold transactions in a comprehensive way. The internal auditor has the option to use any audit methodology.

3.16 During the third quarter of the year, in one of the branches, an auditor observed discrepancies between the locker register balance and the GMS. After a thorough study, management took a view that while no gold was stolen, gold was being unofficially loaned to certain customers. Other practices also favoring certain customer at the cost of the company also came to light. Management came to the view that the branch manager was unaware of these wrongdoings. The branch manager, with a formidable reputation of being control focused, personally did physical verification at the end of every fortnight and tallied the balance with the GMS. It was also observed that there were no discrepancies on those days when he had done the physical verification. The branch manager was admitted that he was not aware of such risks. The management has become wary and wants to know from the internal auditors of other branches on the quality of their assurance.

The Agra Branch

3.17 Agra branch being small, has only one officer trained on GMS. All customers and their employees are personally known to branch staff. During the year, the officer went on two weeks leave. As the branch manager did not know how to use GMS he made manual entries while carrying out transactions. On his return the officer regularized the transactions by passing entries in the GMS and took receipt signatures from the customers once again for the gold delivered on the print out of the electronic delivery note (EDN).

Internal Audit using Traditional Internal Audit Methodology

3.18 The internal auditors have been around for many years and do an in-depth audit during every quarterly visit. They have so far not found any significant observations in their sample depth check. One of their reports did mention that GMS was not used for a fortnight, as the concerned officer had been on leave. Fifty per cent of the audit sample for that quarter included transactions during that period and no discrepancies were observed. The only audit recommendation made was that the other branch staffs be also trained to use GMS.

3.19 In response to the management's year end query, the internal auditors replied that their assurance was based on their sample size and hence be treated as a limited assurance on the compliance of internal controls. However, they agreed with the management's concern and were willing to do an assignment to rule out the possibility of unofficial loans to customers and other irregularities. The procedures involved cross reconciliations including a quantitative reconciliation of gold for the year.

Internal Audit using RBIA Methodology

Stage 1: Assessing Risk Maturity of the Organization

3.20 The internal auditor at the Agra branch started the assignment by asking for the risk maturity assessment done by the internal auditors at the corporate office of ABC and informed that no such assessment was done or required. The branch internal auditor then approached the CFO for his views on the risk management in the company. The CFO replied saying that as per the requirements of Clause 49 of the listing agreement, a risk management committee had been constituted two years ago which met every quarter. A risk management policy had been laid down by this committee and in every meeting, the strategic risks were reviewed and the status reported to the Board through the Audit Committee. With respect to bullion, a reference was made to the Gold Procedure Manual which describes at length the work flow and related internal controls. Also that GMS has a 'no deviation' compliance level status throughout the company as the risk appetite on bullion was zero. The bullion department at the corporate office plans, co-ordinates and monitors bullion activities to ensure that the targets in the business plan are

met. It has an oversight cell on branches which also reviews MIS reports.

3.21 The branch internal auditor wrote back that he had visited the branch, had obtained an overall understanding of the GMS and the controls therein, which, he thought, were impressive. However, he wanted to know whether the risks that these controls aimed to remove were identified, assessed, documented and updated periodically. Based on dialogue with the concerned persons, the branch internal auditor observed that there was no enterprise wide continuous, consistent, structured activity relating to risks, but an occasional discussion on risks followed by a letter to that particular branch. He concluded that the organizational risk maturity was risk aware and submitted this assessment to the Audit committee through the CFO. He recommended that:

- A risk management framework be put in place to implement the risk management policy. This framework (guidelines) would help all managers carry out risk identification, assessment and its response.
- The documentation should result in a risk register.
- Regarding internal audit reports, the branch internal auditor concluded that while he would give an assurance on the compliance of internal controls as per the Gold Procedure Manual and comment on the usage of the GMS, he could not comply with:
  - the HIGH assurance requirement of the Board as there were too many transactions during the year and as per the traditional audit methodology he could at best give a reasonable assurance on controls
  - Nor could he give an assurance that all the significant risks were being managed within the appetite level, i.e., zero, as his audit procedures could not be extended to risks as there was no risk register.

3.22 At the next Audit Committee this report was taken up. The general view of the Directors was that as assurance requirement of the Board was HIGH, an audit report on whether the risks were being properly managed was more relevant than an assurance on whether controls were being followed. Accordingly, the branch internal auditor was requested to undertake a consulting assignment to guide and facilitate the branch management on risk

identification, assessment and response, which was to be completed latest by the end of the second quarter.

Stage 2: Drawing up the Periodic Audit Plan

3.23 For the first two quarters, the branch internal auditor continued to carry out the traditional audit aimed at giving an assurance on controls as per the Gold Procedure Manual. At the beginning of the third quarter, the branch internal auditor reassessed the organization's risk maturity, concluded it as being as risk defined and that RBIA methodology could now be used. The Board's assurance requirements remained HIGH and risk appetite as zero; hence the branch internal auditor had no choice but to include risk responses to all risks (in the risk register) in his audit plan for the last two quarters. He grouped the risks into logical audit groups and allocated appropriate staff. As he was facilitating risk identification, he was well aware of the risk assessment process and its compliance. Hence, he ignored reviewing this aspect. The audit procedures used were to assess risk responses and conclude on the residual risk score (which had to be zero).

Stage 3: Conducting Individual Audits

3.24 During the course of internal audit, instance of non usage of GMS for a fortnight came to the notice of the branch internal auditor. As the GMS is online a comment was made on the weakness in monitoring controls at the Head office. The weakness being non usage of Electronic Delivery Note (EDN) a key control and non usage of GMS had not been brought out by the internal control system. The internal auditor's observation on a weak monitoring control was accepted, and the subsequent action by corporate office was to set up a monitoring control whereby an e-mail was automatically generated from the system listing the names of the branches where no EDN was cut the previous day. Another action was that a pool of staff at the corporate office were trained on GMS and deputed to branches for short durations as temporary staff whenever the concerned officer was on leave.

Response to Management's Year end Query

3.25 The Agra branch management had not identified unofficial gold loans to

customers as a risk. The risk register was updated to include this risk, its response, etc., and the branch manager started an internal exercise for the year to check for any such irregularities. In response to the management's year end query, the branch internal auditors confirmed that risk of illegal gold loan to customers was not recognized as a risk by the Agra branch management, and hence, the response to this was not covered in their internal audit. They accepted this as an audit risk. However, the branch internal auditor asserted that they had given assurance from third quarter onwards on the management of significant risks (as per the risk register) within the tolerance level of zero, which stands as before.

Which Assurance is more Useful to the Board-A Comparison

3.26 On bullion, the Board had a zero risk appetite. The Board would value that internal auditor who can give an assurance on whether the risks are being managed within the zero risk appetite and also is transparent on where his assurance will have an audit risk.

3.27 Following is a comparison of the two internal audit methodologies at the Agra branch.

Table 3: Comparison of the Two Methodologies

Details	Audit under Traditional Methodology	Audit under RBIA (by Branch Internal Auditor)
Does the branch management feel responsible for thinking about risks that could impede its objectives?	✗	✓
Does branch management automatically assume responsibility for verifying that there were no unofficial gold loans for the year gone by?	✗	✓
Does the internal auditor form an opinion on the reliability of the process used by management to identify and assess risks?	✗	✓
Does the internal auditor give a direct assurance on whether the risks are being managed within zero risk appetite?	✗	✓

3.28 Using RBIA, the branch internal auditor is able to give a direct assurance on whether risks are within the zero appetite level or not. Also, they are able to comment on whether the branch management is assessing risks and takes responsibility for managing their risks or not?

3.29 Using the traditional audit methodology, the earlier internal auditor is unable to give a direct assurance on whether the risks at Agra branch are within the zero appetite level or not. Because it is expected that the internal auditors will do an assignment on quantitative reconciliation, it implies that the responsibility of internal controls is not really with the branch management. In that case, the branch management would not be thinking on the new risks in a structured way.

3.30 In the above situation, the internal auditor using RBIA methodology is definitely more useful to the Board.

The Internal Audit Process

4

Four

The Internal Audit Proces

4.1 Internal audit has a planning and execution process through which RBIA methodology is delivered in a consistent manner. It delivers assurance on the management of risks. In the planning process the output is the yearly audit plan, while internal audit reports and tracking outstanding issues with the management is the deliverable in the execution process.

4.2 The planning process starts with the internal auditor becoming acquainted with the business and the industry in which the entity operates. This is a preparatory activity by the auditor to enable him:

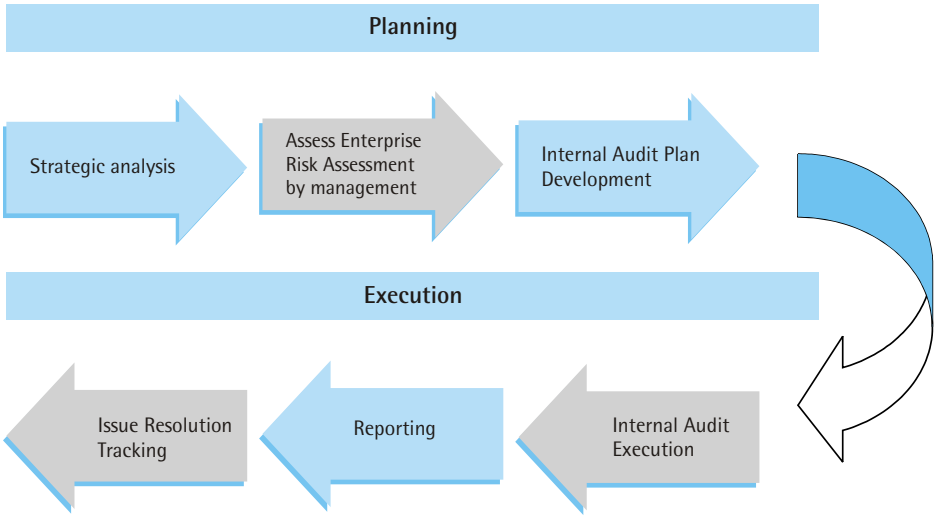
- to assess risk maturity which determines whether to give an assurance using RBIA, and
- to review risk assessment done by management and conclude whether to rely or no to rely on the risk register, and

concludes with identifying auditable units, putting significant risks into audit groups, scheduling the audits, allocating auditors and presenting the yearly audit plan to the audit committee.

4.3 The execution process starts with executing individual internal audits followed with reporting the audit issues and finally keeping a track on management's implementation of accepted issues.

Following is a diagrammatic representation of the process of RBIA.

Figure 2: The Risk-based Internal Audit Process



Planning Process

Phase 1: Strategic Analysis

4.4 In this phase the internal auditor identifies the strategic objectives and understands as to how the organization reacts to challenges. This equips the internal auditor to carry out the risk maturity review and the review of the management's risk assessment.

4.5 Strategic analysis provides a high-level understanding of the organisation's business and the external forces that affect it. The purpose of undertaking such an analysis is that it leads to identification of strategic objectives and understanding of how the organisation reacts to challenges that threaten the attainment of these objectives. The output of this analysis and the information gathered will facilitate understanding of how business risks are linked to the

overall objectives of the organization. This knowledge is used at the risk assessment phase. Strategic analysis is performed using the following information:

- Information on the organisation-Organisation charts, company vision, goals, objectives, strategies, challenges, business plans, and management reports.
- Industry data and reports.

4.6 The following activities are performed during strategic analysis:

- Review and analyse industry information and general business information
- (surveys, industry statistics, publications, etc.).
- Review organisation background information (understanding organisation and operating environment by review of annual report, organisation chart, strategic plans, etc.).
- Conduct interviews with senior management.
- Identify business objectives (Organisation's mission and goals), strategies (how the organisation plans to achieve its missions and goals) and business processes (activities designed to produce a specific output).
- Document the understanding of the business including strategic objectives, key strategies for achieving these objectives, external forces that can threaten the achievement of these objectives and structures and processes to manage such risks.
- Confirm understanding of business objectives, strategies, key risks and process map with the management.
- Periodically update the strategic analysis and take into account the changing circumstances, new management strategies, new risks, etc.

Phase 2: Enterprise Risk Assessment

4.7 In this phase, the internal auditor determines the entity level risk maturity as per the RBIA methodology to arrive at the audit approach and reviews the enterprise risk assessment process by management to conclude whether to rely or not to rely on the risk register. Based on the

audit approach and the reliability of the risk register, the internal auditor identifies the significant risks which are to be audited and need to be taken into the yearly audit plan. The activities undertaken by the internal auditor in this phase are as follows:

A. Assessing the Entity Level Risk Maturity of the Organization and Finalising Audit Approach

The objective of undertaking this activity is to implement Stage 1. The steps involved in this activity are as follows:

Complete out the three stage approach (referred to in to paragraph 3.14 read along with paragraph 2.35 to 2.42 and Appendix 1) and conclude on the entity level risk maturity.

Based on the entity level risk maturity finalise the audit approach (refer to Para 3.9 and Table 2: Audit strategy for different levels of risk maturity.)

B. Reviewing the Enterprise Risk Assessment as Carried out by Management

Under traditional audit, the internal auditor carries out the enterprise risk assessment along with management to arrive at significant risks to be included in the audit plan. However, under RBIA, the assumption is that risk assessment is the responsibility of the management. Hence, the internal auditor evaluates the management's risk assessment to conclude whether to *rely* or *not to rely* on the risk register.

Table 4: Objectives of Enterprise Risk Assessment under Different Audit Methodologies

Methodology	Objective of Enterprise Risk Assessment
Traditional Internal Audit	Carry out the risk assessment along with management to identify significant risks to be included in the audit plan
RBIA	Review the management's risk assessment to decide whether to rely on the risk register. If the risk assessment is reliable and complied with, the internal auditor lists those inherent risks in the risk register which are above the risk appetite as significant risks to include in the audit plan. Where the risk register is not reliable the auditor does not proceed further on the audit under RBIA methodology.

4.8 Prior to preparing the internal audit plan, it is necessary to understanding as to how those risks to which the organisation is exposed have been assessed.to is necessary. Risk Assessment has three processes *viz.* risk identification, risk estimation and risk evaluation.

4.9 Risk Assessment can be defined as the *"overall process of risk analysis and risk evaluation"*. Risk assessment has also been defined as *"identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed"*[4].

4.10 As discussed earlier, there are two categories of risks to which any organisation is exposed to *viz.* external risks and internal risk. No standardized quantitative and/ or qualitative model available to assess both these kinds of risks. This is because even though industry risks to which anorganisation is exposed, may remain constant, the impact that risk would have on each organisation in that Industry differs from one to another. A mix of quantitative and qualitative methods is normally used in risk assessment process.

4.11 An illustrative model process for identifying, estimating and evaluating risks are given in Appendix 1. Under RBIA, the internal auditor compares the organisation's risk assessment process (usually mentioned in the risk framework) with that of the model process to form a view on the design. The next step is to test check, compliance with this process. Based on this, the internal auditor concludes whether to *rely* or *not to rely* on the risk register.

Phase 3: Internal Audit Plan Development

4.12 In this phase, the activity involves putting the significant risks which have been identified during the enterprise risk assessment phase into audit groups, listing out the requests for consulting (internal audit projects) made by management, preparing an internal audit calendar, allocating resources (internal auditors), collating and submitting to the Audit Committee the yearly audit plan for approval. While the yearly audit plan is updated continuously for new risks, quarterly audit plans are frozen and acted upon.

4 Defined by Committee of Sponsoring Organisations (COSO) of the Treadway Commission.

The objective of this phase is to implement the requirements of Stage 2.

Activities Partly Done in Phase 2 of the Internal Audit Process

4.13 The activity in developing an internal audit plan for an entity starts with finalizing the audit strategy which, as mentioned earlier, is derived from the auditor's assessment of the entity's risk maturity.

The next step is to decide whether to *rely* or *not to rely* on the risk register based on the enterprise risk assessment done by management.

4.14 As for different areas of the organization, risk maturity and reliability of the risk register may be different, hence, the objective would be to assess for different areas and business processes the type of assurance that can be given (traditional or RBIA) and internal audit projects (consulting assignments).

Further Activities to Develop a Periodic Internal Audit Plan under RBIA Would Include:

4.15 i. Listing the individual risks to be audited (refer to Para 3.10).

ii. Determining the periodicity (refer to Para 3.11).

iii. Deciding upon auditable units (refer to Para 3.12).

iv. Allocating resources (do limitation management where required).

v. Determining the internal audit plan and obtaining approval of Audit Committee.

vi. Continuously updating the risk and audit universe (say, on a quarterly basis).

An Alternative Approach to Identifying Risks to be Audited

4.16 Another way to determine significant risks is the exclusion method, using the risk register. Out of the above, those risks for which internal audit is not possible or necessary, are removed. Nature of such risks include, risks within the risk appetite, risks that are to be tolerated as they cannot be brought within the risk appetite (other than where contingency plans are required), risks which are examined by third parties (example, external auditors, quality control), satisfactory results in previous internal audit (after considering

changes in the concerned area). The remaining risks shall form the basis of the internal audit plan. These are those on which assurance is required. Also, those risks which may be within the risk appetite but have a high inherent risk score are normally included in the audit plan. Some organisations may need internal audits based on criteria other than risk, such as legal mandate, specific management requests. Business process is the default auditable unit under RBIA and information in the risk and audit universe (RAU) helps in developing an internal audit plan.

4.17 Business process is the *default auditable unit* under RBIA. Key business processes should be included in the internal audit plan. Other processes are also identified for inclusion.

4.18 Individual risks are listed in the risk register and business process to which the risk belongs is mentioned against that risk. Risks relating to a particular activity in a process are put into an *"audit group"*. All the audit related information such as resources allocated, yearly audit plan, issues, issues tracking, etc., end up being entered in separate columns or tables against each risk. Information on risks, processes and audits are now linked across tables. Hence, a resultant database is created and known as the risk and audit universe (RAU). The RAU helps in determining the individual risks to be examined and the audits linked to them. Extracting data from the RAU is the common way to develop an internal audit plan.

Determining and allocating resources-limitation management

4.19 The duration required to complete an internal audit *vis a vis* that the required to complete all audits is estimated and compared with available resources to determine if limitations exist that may hinder the execution of the plan. Management of limitation is done to optimize the resource allocation.

Developing an Internal Audit Plan and Obtain Approval of the Audit Committee

4.20 Proposed internal audit plan should be developed (extracted) from the risk and audit universe (RAU). The proposed internal audit plan should be

presented to the Audit Committee for consideration and adoption. It is often useful to highlight to the Audit Committee the risk areas/ business processes that have been identified to be covered under RBIA, traditional audit and where consulting is suggested and also those which are not being covered with reasons therefor. This information enables the Audit Committee and executive management to make informed decisions on the internal audit coverage and in constructive changes to the internal audit plan.

Updating the Risk and Audit Universe (RAU)

4.21 Such update should be done regularly, say, at least every three months, based on management's reassessment of risks and conclusions from audits during the period. The impact on the audit plan should then be considered. It may be necessary to add audits where new, significant risks have been identified and remove those where risks have been reduced.

Phase 4: Internal Audit Execution

4.22 **In this phase, the internal auditor prepares the internal audit program, detailing the audit procedures to be carried out, carries out the audit procedures, discusses the observations with the auditee and prepares the audit issues.**

The objective of this phase is to implement Stage 3. During the internal audit execution process the following activities are conducted:

Reassessing the Audit Scope

4.23 The internal auditor, by this phase, becomes knowledge able of the organization and its management of risks through the following activities he has undertaken:

- strategic analysis an understanding would have been developed of the objectives, strategies, risks, responses and the overall process map of the organization.
- entity level risk maturity review an understanding of the organisation's risk environment which may be different for areas/ business processes.

- review of the management's risk assessment the reliability of the risk register.

4.24 Before starting any individual audit, the auditor does a diagnostic check specific to that area/business process to see whether the audit scope remains the same or needs to be modified. This diagnostic check includes:

- ***Assignment Level Risk Maturity***

  The internal auditor reassesses the assignment risk maturity to reassess the audit scope.

- ***Business Process Analysis***

  Through a business process review the internal auditor gains a detailed understanding of that particular process under audit and assesses the risks therein and may result in a scope change. This understanding is carried out through interviews and discussions with process owners or control owners. The process understanding should be documented in narrative or through flowcharts and confirmed by the process/ control owners.

Preparing the Internal Audit Program

4.25 The internal audit program consists of two sections, *viz.,*

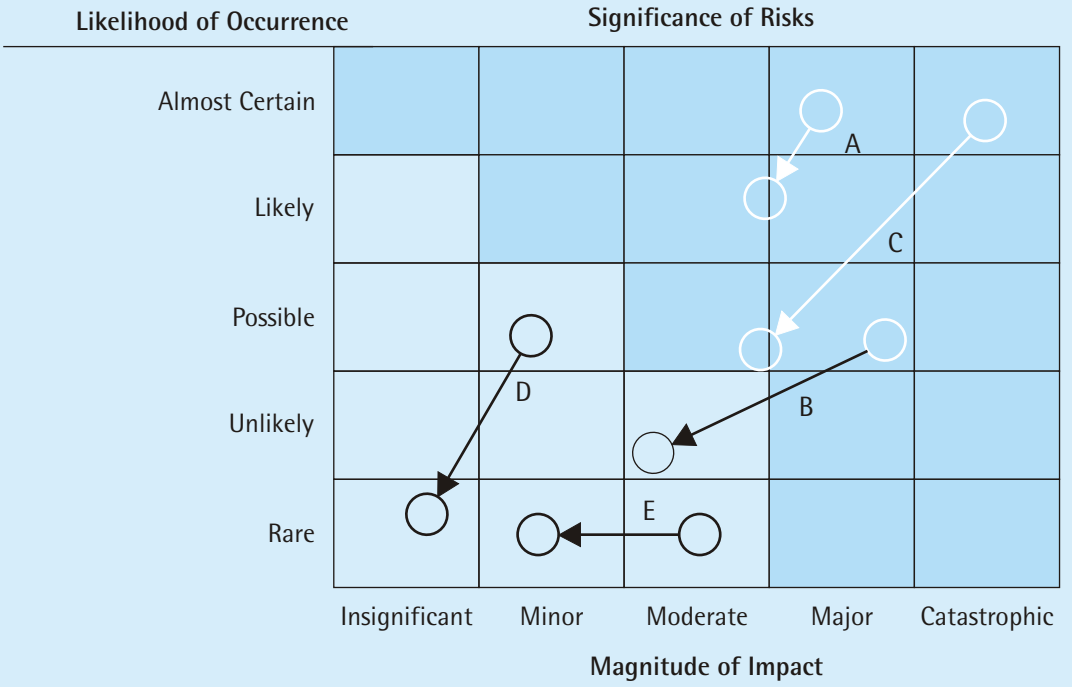
- Where the internal auditor is testing risk management in business processes, the internal audit program will consist of audit procedures to test design and compliance as observing, enquiring, process walkthroughs, depth checks, reviewing monitoring controls, etc.
- Where the internal auditor is testing for the adequacy of the response to risks, the audit procedures to test the internal controls would include verification, recomputation, etc. Prior to that, assessing whether the type of response, such as treat, transfer, tolerate are adequate.

4.26 Usage of the process - risk matrix to determine the areas of emphasis in an audit. Information gained from a number of sources, including strategic analysis, enterprise risk assessment, business process analysis, etc., assist in driving the areas of emphasis in an internal audit program. This is further refined through a process-risk matrix. As illustrated below the process-matrix

helps in understanding the interplay of inherent risks, residual risks, risk appetite, importance of controls, etc.

Table 5: Process Risk Matrix with Inherent and Residual Risk

(Cumulative risks of a business process shown in their inherent and residual state and the length of the arrow shows the control score/importance of controls).



Unacceptable Level of Risk

4.27 This tool can be used either for processes under audit or individual risks in a process. In the above table, business processes under audit are being studied.

- The controls that govern process B move the risks from an unacceptable to an acceptable level. Therefore, testing these controls to determine the effectiveness of the control design is the way forward.

- Process A shows an example of where the residual risks of the process continue to be beyond the risk appetite. This point to the need for either re-evaluation of internal control design or review of the risk response (treat).

4.28 Internal audit procedures on business process audit do not change under RBIA *viz.*,

- Tests of design are associated with internal control design and may be primarily performed during business process analysis. Three types of observations may arize, *viz.*, the process is under-controlled, over-controlled, or inadequately controlled.
- Tests of effectiveness confirm whether key internal controls identified during business process analysis are in existence and are operating as intended.

There may be regulatory compliance issues that also require testing. These issues should be noted in the internal audit program.

4.29 Document evidence, report observations (issues) and update risk register.

- Audit evidence can be physical, documentary, or analytical. The type and source of test evidence obtained and used to complete testing should be documented in the working papers. Each test procedure should link back to the specific scope of internal audit.
- Based on the results of internal audit procedures, observations noted should be documented. Decision is then taken on which observations shall be carried through to the draft report.
- During testing it may be found that while management's view was that internal controls were well designed, it did not address the risk as intended. In this case, management may need to reassess the level of residual risk actually delivered by the internal control and respond accordingly. Risk register should be updated based on necessary changes in assessment of risks and response to it.

Phase 5: Reporting

4.30 In this phase, the internal auditor communicates the audit issues at

different levels of management, obtains the management reply on the proposed action to be taken.

Objective

4.31 The primary objective of reporting is to effectively communicate the results of the internal audit work, thereby helping drive the changes that contribute to the achievement of organizational objectives. Reporting occurs through formal documentation and respective meetings with the process owners, senior management, audit committee and other stakeholders of the audit process.

Reporting Levels

4.32 Strategic-level reports are prepared to communicate the results of work performed to the most senior levels within the organization.

The audience for the process-level reports includes many of the organisation's senior management as well as executive management. Similar to strategic-level reporting, the outputs generated from the process-level activities need to be developed with significant organisation participation and acceptance. In addition to the outputs derived from the process analysis work, as applicable, individual audit reports are also covered.

Internal Audit Report

4.33 The following structure can be used as a basis for internal audit reports. The reporting format used is agreed with the organisation preferably at the inception of audit work.

4.34 *Executive Summary:* An Executive Summary is usually no more than three to four pages with a target audience of senior executives and the 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. *(Refer to Exhibit 7 for a sample report)*

4.35 *Issues:* The purpose of this section is to list the issues to be resolved together with how, when, and by whom they will be resolved. This section would include the issue classification, a brief description, and risk to the organisation, recommendations for resolution, and a management response.

4.36 When applied thoroughly, risk-based internal audit methodology assists in identifying areas of unacceptable residual risk. For departments or subsidiaries within the organisation and auditable processes within that organization, RBIA will provide management with sufficient information to allow them to better optimise and more effectively manage strategic and process risks.

Reporting to Audit Committee

4.37 The internal audit function ultimately reports and is accountable to the Audit Committee. Prior to meeting the audit committee, internal auditors may prepare internal audit reports for the projects performed during the audit cycle and distribute them to the members of the audit committee and other concerned 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.

Phase 6: Issue Resolution Tracking

4.38 **In this phase, the internal auditor tracks the progress of action on the issues where management action was agreed upon.**

Throughout the conduct of internal audit, issues are identified and reported, and ultimately action plans to resolve these issues are agreed to by management. If these action plans are not implemented, the organisation's risk exposure is not sufficiently mitigated and the value of the internal audit function is less likely to be realised. The follow-up process monitors the progress of agreed-upon management action plans and reports this progress to senior management and the audit committee. This phase involves a process to assess management's progress against the agreed-upon action plan and whether these actions were performed adequately and timely.

Following activities are involved in issue resolution tracking:

Determining the Approach

4.39 The audit committee and senior management must support the follow-up process and be willing to intervene in the process when a follow-up action is not being implemented. The method and timing of follow-up and roles and responsibilities should be formally agreed upon with the organization.

Assessing Issue Resolution Activities and Comparing with Agreed Action Plans

4.40 Internal audit should determine whether corrective action was taken and is achieving the desired results, or whether the senior management or the Board has assumed the risk of not implementing the agreed-upon corrective action. In the event that a corrective action has not been taken, written confirmation from management stating that senior management or the Board has assumed the risk of not implementing the agreed-upon corrective action should be taken.

To effectively perform these tasks, following activities need to be coordinated:

- Determining which findings should be followed up.
- Confirming that the reported management response actually occurred.
- Evaluating the reasonableness of management response.

These activities can be performed in conjunction with a scheduled internal audit as per the internal audit plan or as a separate, discrete review. It is important to assess the status of these action plans and the related internal audit test work, as they may affect audits in the current plan.

Reporting

4.41 An issues tracking (or follow-up) report (illustrating the current status of the agreed-upon management action plans) is compiled by the internal auditors. This report allows the Audit Committee and senior management to assess the status of improvements between each audit reporting period. This report may also cover internal auditor's assessment of the effectiveness with which agreed upon action plans are implemented by management.

Some Pitfalls and the Way Ahead

5 Five

Pitfalls During the Assignment

5.1 Some difficult situations which the internal auditor may come across during the course of the assignment are discussed in the following paragraphs.

Lack of Support from Process Owners/ Key Management Personnel:

5.2 Internal auditors quite often face instances of lack of support from process owners. Operational personnel tend consider internal audit as avoidable work as they have different priorities. They may not want to be questioned on the way they manage risks. To minimise such situations, it helps to have the support of those decision makers who are responsible for establishing sound internal controls and an internal audit environment in the organisation. The Chief Internal Auditor may find it useful to promote RBIA and the value it brings to these decision makers with respect to their compliance objectives.

Lack of Proper Communication to the Auditee

5.3 Another common pitfall during internal audit is that the only information the auditee has is the date of the by the internal visit, name of the internal

auditors and copies of earlier reports. It is assumed that the internal audit will be carried out similarly as in the earlier period. This lack of information may result in low cooperation from the auditee. To avoid such scenarios the internal auditor should ensure that:

- Terms of reference and scope of the internal audit are discussed with the responsible management.
- Auditee is informed of the proceedings prior to the field visit.
- Internal auditors are known to be fair in their approach, preparing balanced-view audit reports by including auditee's replies.

Delegation of Internal Audit Planning to Field Audit Team

5.4 It is not an uncommon practice in a multilocational organization for the field audit team to send the audit plan to the principal internal auditor at the head office for approval. This may not be a good practice. At times the internal auditor at field level get caught up in complying with the internal audit manual, completing checklists, meeting personal targets, etc., at the cost of bringing value in the reports. For example, he may not focus on high risk areas or areas which are of importance to management-as risks in critical processes, risks with large control scores, etc., Audit planning hence plays a crucial role to the effectiveness of RBIA. Audit planning cannot therefore be delegated and should be undertaken only by the senior audit team even if it sits at the headoffice.

Misplaced Focus on Risk Scores

5.5 This is common when significant effort has been put in by the organisation during the risk scoring activity at the time of preparation of the risk register. Because of the time constraint the organization may start putting undue reliance on risk scores while for the auditor these scores are indicative and a way to identify significant risks. The internal auditor uses qualitative information to finalise the risks to be considered in the audit plan. Also, at times, he may leave out certain significant risks as they are covered by other auditors. In the above situation, it is important to communicate this aspect so that there is no loss of credibility of the coverage in the internal audit plan.

Other Significant Factors

5.6 RBIA cannot be carried out without interacting extensively with management. Interviewing skills and managing risk workshops are a prerequisite. The internal auditor may need to curb his enthusiasm during these activities and not overstep his role. Also, for both these activities preparation is required, *viz.*

- It is always easier to interview managers if an agenda is circulated in advance. Also, it helps if the discussion is open and the internal auditor avoids trying to direct it. Lastly, the minutes of the interview should also be circulated.
- For risk workshops also, the agenda should be circulated in advance and should be kept simple. Short workshops prove more useful, example, five objectives and 100 minute duration. Using a board or a flip chart for participants to present their view is a standard norm. Minutes should be circulated by the internal auditor within reasonable time. The internal auditor should restrict his role as a facilitator and use the inputs in his audit planning/ fieldwork documentation.

5.7 Internet facilitates the internal audit activity, especially in organizations which are multi locational. Some forward looking organizations already have an internal audit portal as part of their web site. These portals are password protected and contain self assessment questionnaires, working papers, internal audit plan, internal audit reports, issue tracker, etc. It is also possible to conduct an audit under guidance of a senior auditor who is at a different geographical location. Internal auditor need to have strong skills in using web based environment.

The Way Ahead

5.8 Benefits to the management to follow a Risk based internal audit approach in internal auditing are now fairly obvious. Once internal audits based on RBIA is implemented in organizations, the positioning of the internal audit function should improve dramatically.

5.9 The current situation in India is that as RBIA audit approach is in the introduction stage, the skill of the practioner on how he conducts the initial activities in introducing RBIA approach is critical to the acceptance by management. In this regard, following suggestions may be useful:

- Assist the client to develop a risk register and see that it is updated regularly.
- Hold workshops, interviews so that the thinking process also includes risks.
- Assist in preparing a Risk and Audit Universe (RAU).
- Assist the Audit Committee fix the risk appetite by periodically making presentations on:
  - the key risks and the suggested response.
  - the risk assessment processes.
  - risk scores.

Once there is a acceptance by the Audit Committee, it is likely that RBIA would get introduced within the organization.

Exhibit 1

Measurement Yardstick for Likelihood of Risk

Likelihood of Risk Occurrence		
Level	Description	Ranking Criteria
1	Remote	Event may only occur in exceptional circumstances
2	Unlikely	Event could occur in rare circumstances
3	Possible	Event could occur at some time
4	Likely	Event could occur in most circumstances
5	Almost certain	Event is expected to occur in most circumstances

Exhibit 2

Measurement Yardstick for Risk Consequences*

Risk Consequence					
Level	Description	Ranking Criteria	Impact	Resulting in	Illustrations
1	Insignificant	■ < Rs. 50 lakh impact on profitability ■ No impact on market share ■ No impact on reputation	Low	Causes minor inconvenience without impacting the achievement of objectives	■ No potential impact on market shar ■ No impact on brand value ■ Issues would be delegated to junior management and staff to resolve
2	Minor	■ Rs. 50 lakh Rs. 2 crore impact on profitability ■ Consequences can be absorbed under normal operating conditions ■ Potential impact on market share ■ Potential impact on reputation	Low to Moderate	Causes inconvenience without impacting the achievement of objectives	■ Consequences can be absorbed under normal operating conditions ■ There is a potential impact on market share and brand values ■ Issues will be delegated to middle management for resolution
3	Moderate	■ > Rs. 2 crore to Rs 5 crore impact on profitability ■ There is some impact on market share ■ There is some impact on reputation	Moderate	Preventing organisation from achieving some of it's objective for limited period	■ Market share and/or brand value will be affected in the short term ■ The event will require senior and middle management intervention
4	Major	■ > Rs. 5 crore to Rs 10 crore impact on profitability ■ Market share will be affected in the short term ■ Reputation is affected in the short term	Moderate to High	Preventing organisation from achieving majority of it's objective for a long time	■ Serious diminution in brand value and market share with adverse publicity ■ Key alliances are threatened ■ Events and problems will require Board and senior management attention
5	Catastrophic	■ > Rs. 10 crore impact on profitability ■ Serious diminution in reputation ■ Sustained loss of market share	High	Closing down of organisation/ operation or significant part for a long time	■ Loss of key alliances ■ Sustained, serious loss in market share

* The amounts (figures) given in this Exhibit are for illustrative purposes only and are not intended to serve as benchmarks.

Exhibit 3

Measurement Yardstick for Risk Score

Likelihood of Risk	Consequences of Risk				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	5 x 1 = 5	5 x 2 = 10	5 x 3 = 15	5 x 4 = 20	5 x 5 = 25
Almost Certain (4)	4 x 1 = 4	4 x 2 = 8	4 x 3 = 12	4 x 4 = 16	4 x 5 = 20
Almost Certain (3)	3 x 1 = 3	3 x 2 = 6	3 x 3 = 9	3 x 4 = 12	3 x 5 = 15
Almost Certain (2)	2 x 1 = 2	2 x 2 = 4	2 x 3 = 6	2 x 4 = 8	2 x 5 = 10
Almost Certain (1)	1 x 1 = 1	1 x 2 = 2	1 x 3 = 3	1 x 4 = 4	1 x 5 = 5

LEGEND

Risks which require immediate attention

Risks which should be monitored and brought down to green

Risks which do not require action

Exhibit 4

Illustrative Risk Heat Map

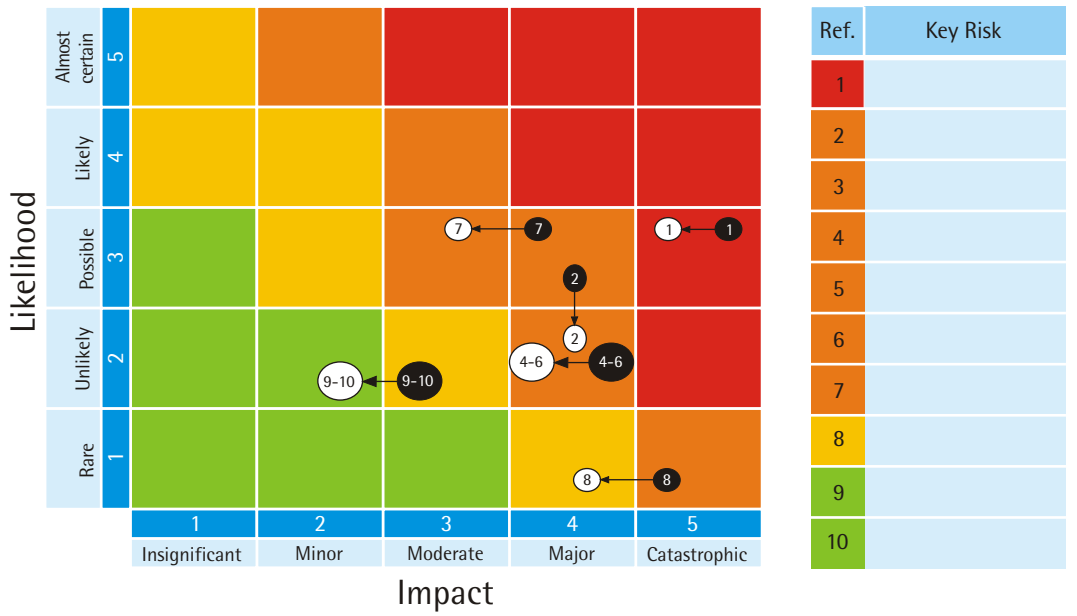


Exhibit 5

Illustrative Risk Register (Part A, B, C)

Part A: Summarised Risk Register

Auditable Unit: Bullion	ABC Bullion Trading Company
Process: Gold Sale	Summarized Risk Register
Sub Process: Order Booking[5]	Serial No of Risk 121-128

Process Objectives	Critical Success Factors	Failure Rate
Sell gold on behalf of Principal at no financial and physical risk to our company	Order booking should consider future risks and treat them at this stage itself	Number of times gold delivery process initiated on the basis of manual instructions i.e., prior to first using GMS software for order booking

Risks which Threaten Objectives	Likelihood	Impact	Controls
Inadequate training provided to employees on the significance of gold procedure manual and its compliance	Possible	Major	New employees receive training as part of orientation process. Existing employees receive periodic compliance training.
At times no trained person on GMS at a branch	Almost certain	Major	Head office maintains a roster of trained persons on GMS who can be deputed for short durations to branches
At times, no action on monitoring reports	Likely	Major	Alerts sent to multiple officers
New risks crystalising without the branch being aware	Possible	Moderate	Quarterly review for updating of risk register

5 As per the Gold procedure manual, when gold is sold on cash basis, the rate is the spot rate. When sold on loan basis the transaction has to be completed and paid for within 21 days of delivery of gold. The bank guarantee submitted should be 110% of the spot rate on loan date. During the loan period the price fixing day is at the choice of the buyer. However once price is fixed the full payment must be credited in the company's bank account on that day itself otherwise bank guarantee is to be invoked the next day.

Part B: Risk Register Showing Inherent Score of Risk

S.No of Risk	Process	Sub Process (Level 1)	Sub Process (Level 2)	Process Owner	Risk	Risk consequence	Gross Risk Assessment[6]		
							Impact	Likelihood	Overall
121	Gold sale	Order booking	Gold to be sold for cash	Bullion Officer	Novice buyer of gold bars	Messy dealings and time wastage of staff as company does not sell less than a gold bar	2 (minor)	4 (likely)	8 (moderate)
122	-do-	-do-	-do-	-do-	Gold rate fluctuates during the day and the rate fixed may not be accepted by Principal	Disagreements with Principal which may result in financial loss and reputation risk	4 (minor)	4 (likely)	16 (catastrophic)
123	-do-	-do-	Gold to be sold on loan basis (delivered now, rate fixed later on, payment recd when rate fixed)	Branch Manager	Buyer may later on default or delay payment	Financial loss to company	4 (minor)	4 (likely)	16 (catastrophic)
124	-do-	-do-	-do-	-do-	Buyer may later on dispute the spot rate fixed	Financial loss to company and reputation risk	4 (minor)	4 (likely)	16 (catastrophic)
125	-do-	-do-	-do-	-do-	Bank Guarantee (BG) expires before receipt of payment from buyer	Financial exposure which may manifest as risk no 123 and 124	4 (minor)	4 (likely)	16 (catastrophic)
126	-do-	-do-	-do-	-do-	BG lower than current spot rate	Financial exposure which may manifest as risk no 123 and 124	2 (minor)	4 (likely)	16 (catastrophic)
127	-do-	-do-	-do-	-do-	BG defective /misplaced	Financial exposure which may manifest as risk no 123 and 124	4 (minor)	4 (likely)	16 (catastrophic)
128	Gold sale	Order booking	All	-do-	Occasional deviation by staff on compliance of gold procedure manual	Financial exposure which may manifest as risks mentioned above	4 (minor)	4 (likely)	16 (catastrophic)

6 Assessing the impact and likelihood of risks has been covered in section on risk estimation below.

Part C: Risk Register Showing Residual Score of Risk

S.No of Risk	Process	Sub Process (Level 1)	Sub Process (Level 2)	Risk	Control	Residual Risk Assessment[7]		
						Impact	Likelihood	Overall
121	Gold sale	Order booking	Gold to be sold for cash	Novice buyer of gold bars	Order booking by only registered customers	2 (Minor)	0	0
122	-do-	-do-	-do-	Gold rate fluctuates during the day and the rate fixed may not be accepted by Principal	Rate fixed by Principal and Rate fixing serial no (RFX) is mentioned in the remittances	4 (Major)	0	0
123	-do-	-do-	Gold to be sold on loan basis (delivered now, rate fixed later on, payment recd when rate fixed)	Buyer may later on default or delay payment	Bank Guarantee of 110%	0	2 Unlikely	0
124	-do-	-do-	-do-	Buyer may later on dispute the spot rate fixed	BG invoked	0	2 Unlikely	0
125	-do-	-do-	-do-	Bank Guarantee (BG) expires before receipt of payment from buyer	Daily monitoring report generated where BG is less than 105% of the closing spot rate for the day. This report is circulated at Branch and Corporate office	4 Major	1 Unlikely	4 Low
126	-do-	-do-	-do-	BG lower than current spot rate	If BG has not yet been invoked thenimmediately invoked	4 Major	1 Unlikely	4 Low
127	-do-	-do-	-do-	BG defective /misplaced	All BG on company's format and kept at safe	4 Major	1 Unlikely	2 Low
128	Gold sale	Order Booking	ALL	Occasional deviation by staff on compliance of gold procedure manual (GPM)	All transactions through a software, viz. Gold management system which has inbuilt internal controls as per GPM	4 Major	0	0

7 Assessing the impact and likelihood of risks has been covered in section on risk estimation below.

Exhibit 6A

List of Information in a Risk and Audit Universe Database (RAU)

The risk and audit universe would typically contain the following information against each risk:

A. RAU - Risk Planning file

Relevant extracts from the risk register (inherent risk details)

1. Process
2. Sub process
3. Risk
4. Gross risk assessment
   - Impact
   - Likelihood
   - Overall score
5. Process owner
6. Risk consequence
7. Adjusted inherent score
8. Control score
9. Last audit
   - Opinion
   - Year
10. Audit Group.

RAU Transaction File for the Year 2007-08

11. Risk
12. Audit group
13. Next audit

- Date
- Man days
- Auditor
- Status
- Risk opinion
- Audit report number.

RAU Issue Tracker File

14. Risk
15. Audit Group
16. Year 2006-07
    - Opinion
    - Tracking status
17. Year 2007-08
    - Opinion
    - Tracking status.

Resource Plan (Q1 of 2007-08)

(For each resource)

18. Auditor
19. Risk
20. Audit group
21. Audit
22. Man days
    - Budget
    - Revised
23. Running calendar.

Exhibit 6B

RAU - Audit Procedures for Risks

S.No of Risk	Sub Process (Level 2)	Risk	Control	Audit Procedure (These procedures are carried out on transactions in GMS)	Score		
					Inherent Risk Score	Residual Risk Score	Control Score
121	Gold to be sold for cash	Novice buyer of gold bars	Order booking by only registered customers	Test GMS to see whether the software takes transactions for unregistered users	8	0	8
122	-do-	Gold rate fluctuates during the day and the rate fixed may not be accepted by Principal	Rate fixed by Principal and Rate fixing serial no (RFX) is mentioned in the remittances	Using CAAT see that against all transactions there is a RFR in GMS. Vouch RFR against the related e-mail/ fax/ letter recd from Principal.	16	0	16
123	Gold to be sold on loan basis (delivered now, rate fixed later on, payment recd when rate fixed)	Buyer may later on default or delay payment	Bank Guarantee of 110% taken and invoked.	Using CAAT list all cases where the transaction has gone beyond 21 days and the BG has not been invoked. Vouch these cases.	16	0	16
124	-do-	Buyer may later on dispute the spot rate fixed	BG to be invoked	Using CAAT list all cases where the payment made by the buyer is at a rate different from RFR. Vouch for reasons.	16	0	16
125	-do-	Bank Guarantee (BG) expires before receipt of payment from buyer	Daily monitoring report listing BG's expiring within 3 days This report is circulated at Branch and Corporate office through e-mail	1. Using CAAT list all cases where BG has expired prior to receipt of payment. Vouch it. 2. Using test pack, create such cases to see whether the case is included in the e-mail	16	4	12
126	-do-	BG lower than current spot rate	Daily monitoring report generated where BG is less than 105% of the closing spot rate for the day. If BG has not yet been invoked then immediately invoked	1. Using CAAT list all cases where BG was lower than spot rate. Vouch it. 2. Using test pack, create such cases to see whether the case is included in the e-mail	16	4	12
127	-do-	BG defective /misplaced	All BG on company's format and kept at safe	Using CAAT obtain a list of all BG. Examine the BGs.	16	2	14
128	All	Occasional deviation by staff on compliance of gold procedure manual (GPM)	All transactions through a software, viz.gold management system (GMS) which has inbuilt internal controls as per GPM	Verify buyer's sign for receipt of gold on electronic delivery challan (EDN)	16	0	16

Exhibit 6C

RAU- Transaction File for the Year 2007-08

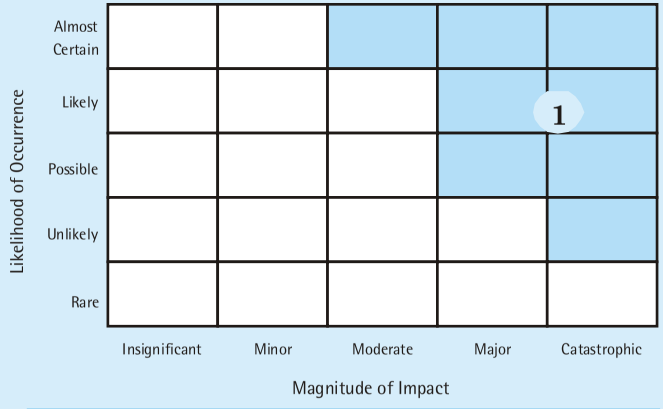
S. No of Risk	Sub Process (Level 2)	Risk	Control	Score			Audit Procedure	2007-08				
				Inherent Risk	Residual Risk	Control		Audit group	Coverage	Auditor Level	Report Date	2006 Opinion
127	Order booking -gold sold on loan basis	BG defective /misplaced	All BG on company's format and kept at safe	16	2	14	Using CAAT obtain a list of all BG. Examine the Bgs.	B14	All Branches	Senior Manager (audit)	Jan 08	Green
128	All	Occasional deviation by staff on compliance of gold procedure manual (GPM)	All transactions through a software, viz. gold management system (GMS) which has inbuilt internal controls as per GPM	16	0	16	Verify buyer's sign for receipt of gold on electronic delivery challan (EDN)	B14	-do-	-do-	Jan 08	Red

Exhibit 7

Internal Audit Report - Executive Summary

AGRA BRANCH - GOLD BULLION TRANSACTIONS			
OBSERVATION	Period	SIGNIFICANCE	PROCESS
1 Electronic Delivery Note not used	Q3/ 2007-08	KEY CONTROL FAILURE	GMS

Risk Map - Audit Issues and Recommendation



AUDIT ISSUE

GMS was not in use for a fortnight as the only trained person, viz. the Bullion officer was on leave. GMS is a risk response to all risks in the gold order fulfillment process as by using GMS all the internal controls automated have necessarily to be followed for each transaction. The Electronic Delivery note (EDN) is a key control as it implies that the transaction has been done through GMS.

AUDIT RECOMMENDATION

As the GMS is online, monitoring of the usage of this control be done whereby an e-mail is automatically generated and received the next day by AGM (Bullion) at Corporate office mentioning the branches where there was no EDN raised the previous day. AGM should enquiry the reasons and take suitable action. Also Corporate office should find a solution whereby there is always a trained person on GMS at branch.

Appendices

Appendix I

Model Process for Assessing and Evaluating Risks

Appendix II

Score Card for Assessing Risk Maturity

Appendix I

Model Process for Assessing and Evaluating Risks

Steps in Risk Assessment

1. Activities in risk assessment can be put in three processes, *viz.*
   - Risk identification.
   - Risk estimation.
   - Risk evaluation.

Risk Assessment Tools

2. Following are some of the popular analytical methods used during risk assessment:
   - Market survey.
   - Dependency modeling.
   - SWOT (Strength, Weakness, Opportunity and Threat) analysis.
   - Event tree analysis.
   - BPEST (Business, Political, Economical, Social and Technological) analysis.

- Fault tree analysis (Root Cause Analysis).
- FMEA (Failure Mode and Effect Analysis).

Risk Identification

3. This is the start point for all risk assessment initiatives. As mentioned earlier all organizations are exposed to varieties of threats and uncertainties which impact the objectives for which they have been established. It is essential that the risk identification process be planned and activities within streamlined. This process should ideally cover all risks and scenarios to which an organization is exposed to during the normal course of its business and also the various business activities which are a source of these risks.

4. Some of the business activities, which are a source of risk, are:

- **Strategic** - These concern the long-term strategic objectives of the organization. They can be affected by capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.
- **Operational** - These concern the day-to-day issues that the organization is confronted with as it strives to deliver it strategic objectives.
- **Financial** - These concern the effective management and control of the finances of the organization and are affected by external factors such as availability of credit, foreign exchange rates, interest rate movement and other market exposures.
- **Human Resources and Knowledge Management** - These concern the effective management and control of the knowledge resources, the production, protection and communication thereof. External risks include the unauthorized use or abuse of intellectual property. Internal risk could be loss of key staff.
- **Compliance** - These concern issues as health and safety, environmental, trade regulations, consumer protection, data protection, employment practices and regulatory issues.
- **Fraud** - All large organizations are exposed to fraud risks. Also various regulatory requirement as Clause 49 require organizations to have sound fraud control mechanisms in place

5. What is the best way to identify these risks? Whether it should be identified by people within the organization? Or external resources who specialize in these areas? Or a blend of both internal and external specialists? Who are the best resources internally to perform risk identification?

   Once again there is no standard practice or guideline which is followed. This decision would depend upon the management, expertise of internal resources, etc. Generally Internal Auditors are considered to be the appropriate personnel to facilitate this activity. Ownership of identifying the risks correctly remains with line management.

   During risk identification care should be taken to identify 'inherent/gross' risk. Rather than concentrating on 'residual/ net' risk. If this is not done the organization will not know what its exposure will be should controls fail. Knowledge on the inherent risk also allows better consideration of whether there is over-control in place if the inherent risk is within the risk appetite, resources may not need to be expended on controlling that risk. Knowledge about both 'inherent' and 'net' risk is important because the extent to which the risk needs to be addressed is informed by the inherent risk whereas the adequacy of the means chosen to address the risk can only be considered when the residual risk has been assessed.

Risk Identification Methods

6. To identify risks one of the following methods are used:
   - Surveys.
   - Interviews.
   - Workshops.

7. Following is the illustrative list of questions which could be used for surveys/ interviews/ workshops:
   - From your perspective, what are your key business and/ or your area objectives?
   - What are some of the significant internal and external risks faced by the organization in the achievement of the business and area objectives?
   - From your perspective what is the likelihood of the risk occurring?

- From your perspective what is the consequence of the risk?
- What are some of the measurable performance targets and key performance indicators (KPIs) that can be linked to monitoring/mitigating the risks identified? (For example Budget to actual, ratings performance ranking).
- What is the frequency of measuring these KPIs?
- What other actions are taken to mitigate/ manage the risks identified?
- What is the frequency of these actions?
- Who is responsible for monitoring these risks?

Industry Risk Models

8. In addition to these generally used methodologies, industry-sector wise risk model can also be used. Generally these models are developed by professional organizations. Industry-sector model is helpful in identifying dynamic risks to which an organization is exposed to.

Which Method to Use ?

9. What is the most effective method or whether a combination of these methods should be used? This depends on various factors including the organizational culture, time available to complete risk identification, etc. Normally this comes with experience to the risk practioner.

Typical Risk Areas

10. Identification of the risks associated with business activities and decision making may be strategic/ tactical, project/ operational. It is important to incorporate risk management at the conceptual stage of projects as well as throughout the life of a specific project.

11. During identification of internal risks it would be important to consider aspects as organizational structure, locations, objectives of the organization, key business processes and functions, strategic partners, outsourced service providers, etc.

12. During identification of external risks the political, economic, social and regulatory aspects in which the organization is functioning needs to be considered. Since identifying external risks is a complex activity generally organizations utilize forecasts and current events/ scenarios. Because of its complexity organization can utilize specialized external sources in this area.

13. An illustrative listing of areas in an organization where risk arises is given below:

Governance	Finance	Operational	Preparedness	Integrity
Authority	Funding	Quality	Morale	Management fraud
Leadership	Financial instruments	Customer service	Workplace environment	Employee fraud
Performance	Financial reporting	Pricing	Confidentiality	Illegal acts
Corporate directionand strategy	Foreign exchange /currency	Obsolescence	Communication flow	Unauthorized use
Incentives	Cash flow	Sourcing	Communication infrastructure	
	Investment evaluation	Product development	Change acceptance	
	Treasury	Product failure	Change readiness	
	Payroll	Business interruption	Challenge	
	Debtor/creditor management	Contingency Planning	Ethics	

Compliance	Environment	Human Resources	Reputation	Technology
Health and safety	Seasonality	Competencies	Brand	Reliability
Environment	Globalization	Recruitment	Reputation	Management information systems
Copyright and trademarks	Competition	Retention	Intellectual property	Access /availability
Contractual liability	E-commerce	Performance measurement	Stakeholder perception	IT security
Taxation	Share price	Leadership development		
Data protection	Strategic uncertainty	Succession planning		

Risk Estimation (or Risk Measurement/ Risk Scoring)

14. Risk estimation can be defined as 'assessing the impact of the risk on the organization.' During risk estimation the following should be kept in mind:
    - Difference between, inherent and residual risk needs to be established.
    - Ensure that there is a clear process methodology on risk estimation so that both likelihood and impact are considered for each risk.
    - Record the estimation of risk in a way which facilitates monitoring and the identification of risk priorities.

15. As discussed earlier all organizations are exposed to various categories and nature of risks, and quantitative methodology may not be sufficient and relevant to complete risk estimation. Hence qualitative characteristics and judgment, knowledge of the management on the organization needs to be utilized (example in the case of reputation risk - a subjective view is all that is possible). Hence risk evaluation is more of an art, than science.

16. Risk estimation can be quantitative, semi-quantitative or qualitative in terms of the probability of occurrence and the possible consequence. The use of a well designed structure is necessary to ensure comprehensive risk identification, estimation and evaluation process. Different organizations will find their own measures of consequence and probability that will suit their needs best. For example many organizations find that assessing consequence and probability as high, medium or low is quite adequate for their needs and can be presented as a 3x3 matrix. Other organizations find that assessing consequence and probability using a 5x5 matrix gives them a better evaluation. If clear quantitative evaluation can be applied to the particular risk - "5x5" matrices are often used, with impact on a scale of "insignificant/ minor/ moderate/ major/ catastrophic" and likelihood on a scale of "rare/ unlikely/ possible/ likely/ almost certain".

Illustrations for measuring probability of occurrence and magnitude of impact of risk (5x5 criteria) are in Exhibit 1 and 2. Also refer to Para 2.4-2.8.

Risk Evaluation

17 When the risk estimation process for each risk has been completed, it is necessary to compare the estimated risks against risk criteria (i.e., risk appetite) which the organization has established. The risk criteria may include associated costs and benefits, legal requirements, socioeconomic and environmental factors, concerns of stakeholders, etc. Risk evaluation therefore, is used to make decisions about the significance of risks to the organization and whether each specific risk should be accepted or treated.

18. A common method of evaluation is to use a 'risk heat map'. The 'risk score' of a risk is the multiple of 'likelihood score' and 'significance score' which is adjusted by the qualitatitive assessment of the management. (Refer to Exhibit 3 for risk score). The risk heat map has likelihood of risks and impact of risks as the two axis and individual risks are plotted on it based on their risk score. Further a "traffic light" approach is used to show the risk, where green signifies do not require action, those which are amber should be monitored and managed down to green if possible, and those which are red require immediate action (refer to Exhibit 4 for risk heat map).

Usage of Risk Scores

19. From the management's perspective when it is reviewing the risk register for CEO/ CFO reporting purposes and giving a disclosure in the Annual accounts on the internal controls, it is not the inherent risk score but the residual risk score which is important; as management wants to assess whether the residual risk is regarded as tolerable, or how far the exposure is away from tolerability.

20. From the internal auditor's perspective it is the inherent risk score which is important as the internal auditor is to give an assurance on the design and adequacy of risk identification process as part of his overall assurance on the risk management process.

Appendix II

Score Card for Assessing Risk Maturity

A. Check list for Assessing Risk Maturity[8]

Risk maturity is the degree to which the organisation understands its risk and has implemented ERM.

a. Understanding on Objectives and their Associated Risks

1. The organisation's objectives are documented and understood.
2. Management has been trained to understand as to what risks are and their responsibilities for them.

b. Installation and Usage of Risk Management within the Organization

3. Process have been defined to determine risks and these have been followed.
4. A scoring system for assessing risks has been defined.
5. All risks have been assessed in accordance with the defined scoring system.
6. Response to the risks have been selected and implemented.

8 Based on An approach to implementing Risk Based Internal Auditing, IIA, UK and Ireland

7. The risk appetite has been defined using the scoring system.
8. Risks have been allocated to specific job titles in the risk register.
9. Management have set up monitoring controls on processes, responses and action plans.
10. Risks are regularly reviewed by the organization and the risk register updated.
11. Management report risks to Directors where responses have not managed risks the risks to a level acceptable to the Board.
12. All significantly new projects/ products are routinely assessed for risks.

c. Assessment on Managers Understanding and Usage of Risk Management

13. Responsibility for determination, assessment and management of risks is included in job description.
14. Managers provide assurance on the effectiveness of their risk management.
15. Managers are assessed on their risk management performance.

B. Suggested Scoring and its Interpretation

Score

0 - No

1 - Yes, Incomplete/ Possibly

2 - Yes.

Conclusion on Risk Maturity

0	-	7	:	Risk Naïve
8	-	14	:	Risk aware
15	-	20	:	Risk defined
21	-	25	:	Risk managed
26 and above			:	Risk enabled.

www.icai.org

The Institute of
Chartered Accountants of India

P O Box No. 7100, Indraprastha Marg
New Delhi - 110 002 INDIA

18 I A C 0 0 1 1