Technical Guide on Risk Based Internal Audit

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

Technical Guide on Risk Based Internal Audit

Internal Audit Standards Board

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

New Delhi

DISCLAIMER: The views expressed in this Guide are those of author(s). The Institute of Chartered Accountants of India may not necessarily subscribe to the views expressed by the author(s).

Basic draft of this publication was prepared by CA. Nikhil Kenjale, CA. Madhavi Bhalerao, CA. Sandeep Kunte, CA. Sameer Karyekar, CA. Ashish Athalye, CA. Anuja Ramdasi and CA. Sonali Vidhate.

First Edition	:	November, 2007
Second Edition	:	March, 2026
Committee/Department	:	Internal Audit Standards Board
Email	:	iasb.secretariat@icai.in
Website	:	www.icai.org
Price	:	₹ 200/-
ISBN No.	:	978-93-47892-02-8
Published by	:	The Publication Department on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110 002 (India)
Printed by	:	Friends Digital Color Print Shop Nehru Place, New Delhi - 110 020 (India)

Foreword

The profession of internal audit has witnessed a profound evolution in recent years shaped by rapidly changing business environment, heightened expectations of stakeholders and increasingly complex risk landscapes. In this dynamic context, internal audit has moved beyond its traditional control focused role to emerge as a strategic function with Risk-Based Internal Audit (RBIA) becoming central to delivering forward-looking insights and value.

The Institute of Chartered Accountants of India (ICAI) had issued Technical Guide on Risk-Based Internal Audit in 2007, which served the profession well over the period. Since then, however, the business and regulatory ecosystem has undergone significant transformation. The advent of disruptive technologies, such as data analytics, artificial intelligence and automation, along with increasing globalization and cross-border operations, has fundamentally altered the very nature of risks faced by organisations. Additionally, the instances of global frauds and financial reporting irregularities have further heightened expectations from internal auditors to provide deeper insights and timely risk indicators. At the same time, evolving regulatory and compliance requirements, both In India and globally, have considerably expanded the scope and responsibilities of internal audit functions.

In light of these developments, ICAI though its Internal Audit Standards Board (IASB) has undertaken a comprehensive revision of the Guide to align it with contemporary practices and evolving stakeholder expectations and incorporating the requirements of the revised Standards on Internal Audit (SIAs) issued in February 2026. This Technical Guide has thus been updated to provide practical guidance enabling members to adopt a structured, risk-focused approach in diverse and evolving organizational environments.

I place on record my appreciation for CA. Ravi Kumar Patwa, Chairman, CA. Sridhar Muppala, Vice-Chairman and all the members of the Internal Audit Standards Board of ICAI for their leadership, vision and commitment in bringing out this timely publication.

I am confident that the revised edition of this Technical Guide will serve as a valuable resource for members, enabling them to adopt a proactive, insightful and future-ready approach to internal auditing and to contribute meaningfully to strengthening organizational governance and resilience.

March 24, 2026
New Delhi

CA. Prasanna Kumar D
President, ICAI

Preface

Risk management has become an integral component of organizational governance and internal audit plays a pivotal role in evaluating and strengthening risk management frameworks. With growing expectations from stakeholders, regulators and those charged with governance, internal auditors are increasingly required to adopt a structured and risk-focused approach in planning and executing their assignments. This has led to the wider adoption of Risk Based Internal Audit as an effective methodology for delivering value-driven assurance.

The Internal Audit Standards Board of the ICAI issued a Guide on Risk-based Internal Audit in 2007. Since then, the business and regulatory environment has undergone significant transformation, necessitating a comprehensive revision of the Guide to address emerging challenges and evolving expectations from the internal audit function. This Technical Guide seeks to provide clarity on key concepts and practical aspects of Risk Based Internal Audit through a structured and application-oriented approach.

This Technical Guide comprehensively addresses key aspects of Risk Based Internal Audit, including understanding organisational risks and internal controls, evaluating risk management processes, developing the audit universe, planning and execution of Risk Based Internal Audit engagements and reporting. It also elaborates on the role of internal auditors in assessing the effectiveness of risk management frameworks while preserving independence and objectivity.

We express our sincere gratitude to CA. Prasanna Kumar D, President, ICAI and CA. Mangesh Pandurang Kinare, Vice-President, ICAI, for their leadership, guidance and continued encouragement in advancing the work of the Internal Audit Standards Board.

We also express our sincere gratitude to the Central Council Members for their support and guidance in finalizing this Technical Guide. We place on record our appreciation to all the members of the Board for their valuable contributions, insightful deliberations, strategic input and unwavering commitment demonstrated throughout the development of this Technical Guide.

We place on record our appreciation for the significant contribution made by all the members of the study group whose expertise and commitment have materially contributed to the development of this Technical Guide. The Board also acknowledges the valuable input received from reviewers and subject matter experts.

We further acknowledge the dedicated efforts of CA. Arti Bansal, Secretary and CA. Ranjit Mahto, Internal Audit Standards Board in coordinating the Study Group meetings, consolidating input and facilitating timely completion of this Technical Guide.

We are confident that this Technical Guide will serve as a practical reference for members engaged in internal audit assignments across sectors and will support them in strengthening risk assessment and audit effectiveness.

CA. Ravi Kumar Patwa
Chairman
Internal Audit Standards Board, ICAI

CA. Sridhar Muppala
Vice Chairman
Internal Audit Standards Board, ICAI

March 24, 2026
New Delhi

Foreword to the First Edition

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.

November 2, 2007
New Delhi

CA. Sunil H. Talati
President, ICAI

Preface to the First Edition

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 decision making, 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.

November 5, 2007
Kolkata

CA. Abhijit Bandyopadhyay
Chairman, Committee on Internal Audit

MEMBERS OF THE COUNCIL [2025-29]

CA. Prasanna Kumar D, President

CA. Mangesh Pandurang Kinare, Vice President

CA. Agarwal Vishnu Kumar

CA. Chhaira Jay Ajit

CA. Chhajed Piyush Sohanrajji

CA. Chitale Chandrashekhar Vasant

CA. Doshi Vishal

CA. Kabra Arpit Jagdish

CA. Durgesh Kumar Kabra

CA. Khandelwal Purushottamlal Hukamichand

CA. Charanjot Singh Nanda

CA. Savla Priti Paras

CA. Sharma Umesh Ramnarayan

CA. Babu Abraham Kallivayalil

CA. Dayaniwas Sharma

CA. Madhukar Narayan Hiregange

CA. Muppala Sridhar

CA. Rajendra Kumar P

CA. Sripriya K

CA. Patwa Ravi Kumar

CA. Sanghi Sanjib

CA. (Dr.) Agarwal Rohit Ruwatia

CA. Chhajed Abhay

CA. (Dr.) Goyal Anuj

CA. Gupta Satish Kumar

CA. Misra Gyan Chandra

CA. Shah Pankaj

CA. Agarwal Sanjay Kumar

CA. Chugh Hans Raj

CA. Jain Pramod

CA. Sharma Rajesh

CA. (Dr.) Singhal Sanjeev Kumar

Joint Secretary, MCA

Shri Bala Murugan D.

Shri Manoj Kumar Sahu

Shri Naveen Singhvi

Shri Sanjay Sharan

Justice (Former) Shashi Kant Gupta

Shri Mukhmeet Singh Bhatia

Shri Vinod Kumar Jindal

MEMBERS OF THE INTERNAL AUDIT STANDARDS BOARD, ICAI
[2026-27]

Members from the Sitting Council

CA. Ravi Kumar Patwa, Chairman

CA. Sridhar Muppala, Vice-Chairman

CA. Arpit Jagdish Kabra

CA. Chandrashekhar Vasant Chitale

CA. Durgesh Kumar Kabra

CA. Jay Chhaira

CA. Priti Paras Savla

CA. Rajendra Kumar P

CA. Sripriya Kumar

CA. Abhay Chhajed

CA. Pankaj Shah

CA. Charanjot Singh Nanda

CA. Rajesh Sharma

Shri Mukhmeet Singh Bhatia

Co-opted Members

CA. Subhash Chandra Saraf

CA. Ankitkumar Nathabhai Chotaliya

CA. Parin Vijay Shah

CA. Om Prakash Loya

CA. Srinivas Puligilla

CA. Viswanath K

CA. Mohit Kumar Dhand

Acknowledgement

The Board acknowledges the contribution made by the following members of the Study Group constituted for the purpose of revising Guide on Risk Based Internal Audit and we place on record our gratitude for their contribution in enrichment of knowledge of the members.

Study Group Members:

- CA. Nikhil Kenjale, Pune
- CA. Madhavi Bhalerao, Pune
- CA. Sandeep Kunte, Pune
- CA. Sameer Karyekar, Pune
- CA. Ashish Athalye, Mumbai
- CA. Anuja Ramdasi, Pune
- CA. Sonali Vidhate, Pune

Experts/ Reviewers:

- CA. Nehal Shah, Mumbai
- CA. Niraj Kumar, Gurugram
- CA. Deepti Rathor, Mumbai
- CA. Chirag Bakshi, Vadodara
- CA. Mahavir Jain, Bhilai
- CA. Pritesh Mashru, Ahmedabad
- WIRC of the ICAI

Abbreviations

RBIA	Risk Based Internal Audit
CAE	Chief Audit Executive
ERM	Enterprise Risk Management
SIAs	Standards on Internal Audit
MD&A	Management Discussion & Analysis
RMF	Risk Management Framework
KPI	Key Performance Indicator
IT	Information Technology
ESG	Environment, Social & Governance
TWCG	Those Charged with Governance
RMS	Risk Management Standards
NIST	National Institute for Standards and Technology
U.S.	United States

Contents

Chapter 1
Introduction

Evolution is continuous. The Institute of Chartered Accountants of India ("ICAI") had issued a Technical Guide on Risk-based Internal Audit in the year 2007. Since the issuance of the said Guide, there has been considerable shift in the way the businesses are conducted, nationally and internationally. Hence there was need to revise this Guide.

Notable Milestones

1.1 Some of major developments that necessitated revisions of this Technical Guide include:

- **Disruptive Technologies:** Technology advancement has led to the dispensation of all the knowledge stream boundaries and the manual efforts. Artificial intelligence, Internet of things (IOT), block chain, Robotic Process Automation (RPA) are some the technologies which are redefining the business. This is supported by the advancement in the cloud systems pushing the organizations to move away from the product purchase model to the subscription model (popularly known as SaaS model).
- **Global Footprint:** It is increasingly becoming important for Corporates to have a comprehensive view of geography-wise laws in which they operate. Large conglomerates have subsidiary, parent relationships across the borders and the world activities are coming closer.
- **Ever Changing Business Model:** Business models are evolving and changing rapidly eventually encountering newer risks, which need to be addressed effectively.
- **Disruptions:** The COVID pandemic has changed the way businesses were done. More and more online platforms and tools have emerged and business models have undergone a major shift. Business trend is moving from B2B to B2C model. The audit methodologies have also changed and remote auditing has become an acceptable way of audit. These changes have brought in more opportunities vis a vis challenges and risks.

- **Global Frauds/ Financial Reporting Irregularities:** Corporates started facing newer risks and threats like cyber-attacks, data privacy breaches, etc. leading to new challenges in managing risks. The magnitude of online frauds has increased exponentially. The global cost of online payment fraud is expected to reach US$362 billion by 2028 (Source: Juniper Research report on online payment fraud from November 2022). Also, corporates continued to witness frauds, especially because of management override of controls leading to undertaking unethical transactions, approving transactions by the authorities who had self-interest and fraudulent financial reporting.
- **Additional Compliance:** The overall situation and complex business models have led to the introduction and implementation of legislations that would help to prevent or detect these irregularities in a timely manner and on an overall level improve the Corporate Governance. This included prescribing stringent norms for Governance, Risk and Controls and heightened expectations from those charged with the governance (TCWG). Specific legislations included the following:
    - Explicit requirements about internal audit applicability under section 138 of the Companies Act, 2013 and Companies (Accounts) Rules, 2014.
    - Introduction of Internal Financial Controls requirements through Section 134 (5) of the Companies Act, 2013. This requires Directors to explicitly state their responsibilities in terms of reliable financial reporting and adequacy of Internal Financial Controls of the Company.
- **Other Regulatory Changes/ Requirements:**
    - Issuance of Standard on Auditing (SA) 610 (Revised) Using the Work of Internal Auditors – applicable for financial statements beginning on or after 1 April 2016 – this includes option for the statutory auditors to obtain direct assistance from the internal auditors [Important to note the relationship between SA 315 and SA 610 (Revised)].
    - CARO 2020 restoring the requirement whereby the statutory auditors have to comment on “Does the company have an internal audit system in accordance with its size and business

activities. Have the reports of the internal auditors been considered by the statutory auditor."

- The Securities and Exchange Board of India through its Listing Obligations and Disclosure Requirements) (LODR) Regulations, 2015; w.e.f. 30 Jun 2021 has mandated Top 1000 listed entities to confirm whether they have complied with the risk management committee requirements.
- The Reserve Bank of India vide its circular DoS.CO.PPG./SEC.04/11.01.005/2020-21 dated January 07, 2021 has supplemented a mandate for all scheduled commercial banks to have a Risk Based Internal Audit (RBIA). Further, through its notification RBI/2020-21/88 Ref.No.DoS.CO.PPG./SEC.05/11.01.005/2020-21 dated February 03, 2021, it has mandated RBIA to the prescribed Non-Banking Financial Companies and Primary (Urban) Co-operative Banks (Source: https://www.rbi.org.in).

The above list is only an indicative one and merely attempts to cover important changes in the legal requirements in the recent past.

1.2 It is important for the internal auditors to redefine their internal audit strategies and processes in order to continue to add value to their clients or stakeholders.

This Technical Guide on Risk Based Internal Audit, therefore, elaborates on all the fundamental aspects of the Risk Based Internal Auditing by way of discussion on basic concepts or definitions, examples and diagrams considering the above changed scenario.

Chapter 2

Fundamentals of Risks and Risk Based Internal Audit (RBIA)

Preface to the Standards on Internal Audit

2.1 Framework governing internal audits issued by the ICAI defines internal audit as:

> "Internal audit is an independent objective assurance and advisory function that evaluates the effectiveness of an organization's governance, risk management, compliance and control processes by adapting a systematic and disciplined approach to add value and provide insight and recommendations to improve the efficiency of the organization's operations, as may be required in terms of scope of works."

Therefore, in order to put the definition in action, one needs to understand:

(i) **Independence**

Independence of the internal audit function refers to the organizational positioning and conditions that enable the internal auditor to carry out assigned responsibilities in an objective manner. Independence is achieved through appropriate reporting relationships, scope clarity and safeguards that prevent undue influence on the internal auditor's judgement. While the manner of achieving independence may vary depending on the size, structure and nature of the organization, the internal audit function should be positioned such that it can perform its responsibilities objectively, free from interference in determining the scope of work, performing audit procedures and communicating results.

(ii) **Objectivity**

Objectivity denotes an impartial and unbiased mental attitude that enables internal auditors to perform engagements with professional integrity, without allowing conflicts of interest or undue influence to compromise professional judgment.

(iii) **Assurance**

Assurance represents an independent and objective evaluation of evidence to provide reasonable confidence to stakeholders regarding the adequacy, effectiveness and reliability of governance, risk management, compliance and control processes.

(iv) **Advisory Function**

The advisory function comprises the provision of insights, advice and recommendations designed to enhance organisational processes and performance, without the internal auditor assuming management responsibilities or impairing independence and objectivity.

(v) **Internal Controls and Risk Management**

Internal controls and risk management constitute integral components of management functions and business operations. The internal auditor is expected to evaluate the design, implementation and operating effectiveness of internal control and risk management processes, including related reporting mechanisms, as established by management.

(vi) **Governance**

Governance refers to the framework of relationships among the organisation, its Board, management and other stakeholders, through which organisational objectives are established, achieved and monitored. It encompasses compliance with internal policies and procedures, as well as applicable laws and regulations.

(vii) **Compliance**

Compliance refers to adherence to applicable laws, regulations, standards, internal policies, procedures and contractual obligations governing the organisation's activities.

(viii) **Systematic and Disciplined Approach**

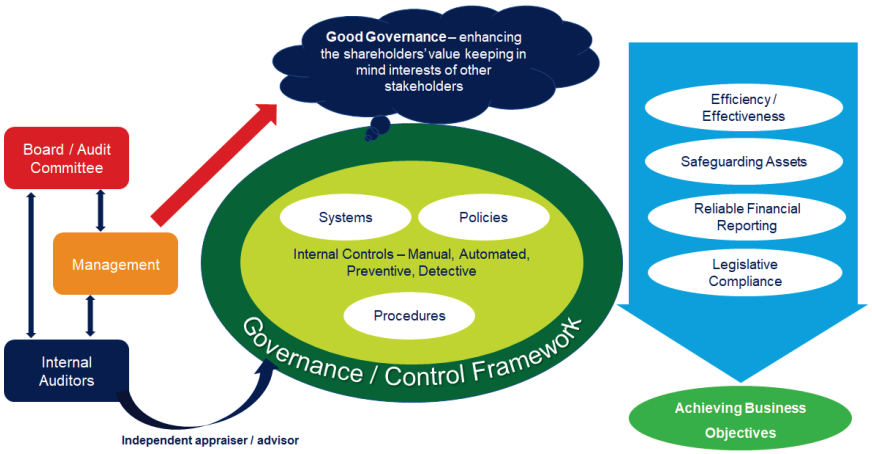
A systematic and disciplined approach denotes the structured and consistent methodology adopted by internal audit in planning, executing, documenting and reporting engagements in accordance with applicable professional standards.

(ix) **Value Addition**

Value addition refers to the contribution of internal audit in enhancing organisational effectiveness by improving governance, risk management and control processes and supporting informed decision-making. Value addition also includes suggestions for increasing performance, reduction in cost and increment in services.

(x) **Organisational Objectives**

Organisational objectives represent strategic, operational and future oriented goals of the organisation, reflecting the interests of relevant stakeholders and the conduct of its operations. These objectives can be understood from vision- mission statement, long or medium plans, annual plans.



Understanding Risk in the Context of Business

2.2 In order to understand RBIA, it is essential to understand the concept of risk and its relationship with the internal control. As mentioned above, anything that creates an obstacle in achieving the business objectives is a risk and is required to be managed. Therefore, the risk could be a negative outcome for the business, or it could be a cost of opportunity lost.

Let us look at a mathematical equation to understand how risks and internal controls are related to each other.

INHERENT RISK (minus) INTERNAL CONTROL = RESIDUAL RISK/ EXPOSURE

Let us assume that the risks and internal controls can be cardinally measured. Logically and mathematically, three scenarios are possible:

Sr. No.	Inherent Risk	Internal Control	Residual Risk	Remarks
1	100	0	100	It is a PURE RISK situation where there are no internal controls.
2	100	< 100, say 80	< 100, it will be (100 – 80 = 20)	Usually it is a common situation in every organization as risk cannot be fully eliminated.
3	100	> or = 100	NIL (It cannot be negative)	These situations can only exist in theory alone as there is no organization with a zero risk.

Higher the level of internal control, lesser would be residual risk and *vice versa*. Also, with higher level of internal controls, at times, there would be lesser convenience allowed to the users in undertaking business activities.

Most of the organizations will get classified under Sr. No. 2 above. Therefore, control environment is better understood by the level of residual risks they carry at any given point in time.

Though, in practice, it is difficult to put the cardinal measurement to the risks and internal controls, there is a good amount of research which has happened on this topic to objectively measure risks and residual risks.

Different Criteria to Assess and Manage Risk

Risk Appetite

The level of risk an organisation is willing to accept in pursuit of its objectives E.g. An organization will not have a plant in a geography that is prone to floods.

Risk Tolerance

It is often a sub-set of Risk appetite and it is defined at a level which will enable an organization to objectively measure the risk involved in the given business context. E.g. The company will go ahead to have its plant in a geography where the rainfall is between 800 to 1300 mm in a year. Another example could be a manufacturing plant may accept the quality of a batch of production if the failed products are in the defined parameters say 0.5%.

Risk Impact

It an outcome after the risk event has happened. E.g. The interest loss because of keeping the funds idle for 1 month in the Company's treasury pool amounting to Rs. 30 Cr.

Risk Possibility

At times used as a synonym with "Risk Probability" or "Risk Likelihood" and it defines the chance of risk event occurring. E.g. Chance of an earthquake in the locations where the Company operates which will lead to business disruption i.e. Risk impact

Risk Velocity

It is a time gap between event's occurrence and its impact. It has two sub-sets name 'speed of reaction' and "speed of recovery" that is restoring the normal business situation after a risk event has happened. For example, the time taken to switch over business operations from live environment to the backup site will be "speed of reaction" and the time taken to restart the operations again from the earlier affected live environment will be "speed of recovery". The concept of Business Continuity Planning and Disaster Recovery Planning are related to these terminologies respectively.

Risk Interdependency

Risk is better understood by its relationship with the other risks. E.g. Manpower attrition risk leads to other set of risks like disruption, delays in executing projects, higher recruitment costs etc.

Frequency

How frequently (i.e. expected occurrence of risk events) the risk would occur and impact the organization. E.g. Earthquakes in Japan are frequent than in India.

Vulnerability

It is a measure as to how susceptible the organisation is to a given risk. Greater the vulnerability, greater is the risk. E.g. the organisation is vulnerable to cyber risks if it has inadequate network security.

Chapter 3

Risk Management and the Role of Internal Auditor in Risk Management

As per SIA 150, Risk Management as issued by the ICAI.

3.1 Risk Management is defined as a process:

- With a series of steps, taken on a continuous basis to identify the threats and vulnerabilities, assess them for severity and likelihood, monitor risks, prioritize them for action and to minimize their possible negative impact through mitigation actions.

Risk Management is an attempt to minimize the number of surprises, enabling the organization to:

- Exploit opportunities when they arise and
- Be prepared for potentially damaging events and circumstances when they actually materialize.

The main objective of the Risk Management is to help an organization to achieve its strategic goals and not always to eliminate or even minimize the risks. The primary objective is to identify, assess and understand risks so that the management can take informed decisions (popularly known as "risk response") and monitor them effectively.

Organizations face risks - internal and external. In an organization who has got a multi-continental presence, possible risks and management measures could be as follows:

Risks	Possible Risk Mitigation Measures
Customer concentration	• Diversify the customer base • Research/ innovation to enter into new industry/ product segments
Foreign currency rate fluctuation	• Evaluate possibilities of achieving natural hedge E.g. offsetting US $ outflow obligations with US $ inflows • Obtaining hedging covers like options, forward contracts etc.

Non-compliance with applicable laws	• Engaging experts especially at foreign locations where understanding the land laws is a challenging task. • Automation of compliance process to get timely update of level compliance achieved/ not achieved.
Employee attrition	• Better compensation structuring • Launching employee career advancement schemes/ trainings • Better employee engagement measures – cultural events, work-life balance initiatives etc.
Cultural differences	• Employee training and cultural exchange programs • Local recruitment strategy

The above list is indicative and real examples can be easily gathered from the annual reports published by the listed entities.

It is important to know that Risk management is applicable at the **Micro level** that is transaction level (e.g. internal controls which are established for ensuring accuracy of data entry and avoid invalid data being entered into an accounting system) as well as at the **Macro level** i.e. at an entity level. When risk management is applied at an entity level, it is commonly known as **Enterprise Risk Management (Enterprise Risk Management).**

Risk Management Framework is the combination of structure, systems and processes put in place to organise the various risk management activities and to integrate them seamlessly into the organisation. Risk management activities, forming part of the framework, are designed to enhance the organization's ability to, amongst others:

(a) Provide strategy, leadership and direction on risk management.

(b) Establish a culture of risk awareness and management throughout the organization.

(c) Provide an organization structure for assigning risk management resources and defining their roles and responsibilities.

(d) Capture and maintain a comprehensive database of all risks with periodic updation of risk inventory.

(e) Ensure **expertise and competence** in the area of risk management.

(f) Exercise **continuous monitoring** and **oversight** on risk management.

(g) Identifying areas where Internal Controls are weak or impaired, which leads high risk to the business.

(h) Categorise risk based on organisation's risk policy.

(i) Periodic communication of risk management matters and formal reporting of risk status to management and those charged with governance. (Ref: Para 4.3 of SIA 150).

Enterprise Risk Management is a term used to refer to various risk management frameworks uniformly applied on an entity-wide basis towards a comprehensive approach to manage organisational risks. As per the SIA 150, Risk Management issued by Internal Audit Standards Board of the ICAI.

Risk Management and Enterprise Risk Management

While both, Risk Management and Enterprise Risk Management, aim to identify, assess and mitigate risks to an organization; they differ significantly in their methodologies and outcomes.

- Risk Management is considered more at functional or departmental or unit level; whereas Enterprise Risk Management is spread across the entire organisation.
- Enterprise Risk Management is much wider concept that encompasses aspects related to various levels and layers of the organisation viz. unit, division, branch, subsidiary companies and the entire entity.

Although there are various Risk Management standards available in general and for an industry in particular, the underlying principles are generally similar in nature.

Risk Management Requirements

Securities and Exchange Board of India

3.2 As far as Indian Corporate context is concerned; the terminology Risk Management has been referred to in LODR requirements and Companies Act 2013. Market regulator SEBI has published the SEBI (LODR) (second amendments) vide notification No. SEBI/LAD-NRO/GN/2021/22 on 5 May 2021. With the introduction of key amendments in SEBI (LODR) regulations, the regulator has emphasised the need of holistic risk management to

improve corporate governance standards of listed companies in India. The regulations require that the top 1000 listed companies, determined based on certain laid down criteria, should formulate the Risk Management Policy and constitute Risk Management Committee to supervise and oversee the Risk Management practices of the organisation. Section 134(3)(n) of the Companies Act, 2013 requires the Board of Directors to include in their report to the shareholders, a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company.

Companies Act, 2013

Subsection (1) and (4) of Section II of Schedule IV of Companies Act, 2013 on "Code for Independent Directors", role and function require them to:

(1) help in bringing an independent judgment to bear on the Board's deliberations especially on issues of strategy, performance, risk management, resources, key appointments and standards of conduct.

(4) satisfy themselves on the integrity of financial information and that financial controls and the systems of risk management are robust and defensible.

The overall responsibility for developing, implementing and monitoring of risk management rests with the Board of Directors, Risk Management Department and the Management. It is expected that these aspects should be appropriately covered in the internal audit scope.

Thus, there is variety of literature on the Risk Management and Enterprise Risk Management in the global and Indian context. Although there are differences in the terminologies of Risk Management and Enterprise Risk Management, in this Technical Guide they have been used interchangeably since the main focus of this Guide is to provide guidance to the members as to how the RBIA approach is followed when the organization has some kind of risk management practices. This Guide as well as the other SIAs provide guidance as to how the Internal Auditor should handle the situation where there is no risk management framework established in the organization also the situation where an effective Enterprise Risk Management framework is established.

Risk Management and Corporate Governance

3.3 Standard on Internal Audit (SIA) 150, "Risk Management," defines risk as a threat exploiting vulnerability of business assets or processes or controls by occurrence of an event which could prevent the organization from achieving its goals and objectives or which can significantly impact the business operations, internal controls and business continuity of the organization. Areas which can be impacted by risk are broadly classified into strategic, reputational, operational, financial, legal, environmental, etc.

The aim of Corporate Governance is to ensure that the interests of all the stakeholders remain in balance with transparency and accountability. Risk Management plays a major role in Corporate Governance.

SA 315, Identifying and Assessing the Risk of material misstatement through understanding the entity and its environment.

The entity conducts its business in the context of industry, regulatory and other internal and external factors. To respond to these factors, the entity's management or those charged with governance define objectives, which are the overall plans for the entity. Strategies are the approaches by which management intends to achieve its objectives. The entity's objectives and strategies may change over time.

Business risk is broader than the risk of material misstatement of the financial statements, though it includes the latter. Business risk may arise from change or complexity. A failure to recognise the need for change may also give rise to business risk. Business risk may arise, for example, from:

- The development of new products or services that may fail;
- A market which, even if successfully developed, is inadequate to support a product or service; or
- Flaws in a product or service that may result in liabilities and reputational risk.

An understanding of the business risks facing the entity increases the likelihood of identifying risks of material misstatement, since most business risks will eventually have financial consequences and, therefore, an effect on the financial statements. However, the auditor does not have a responsibility to identify or assess all business risks because not all business risks give rise to risks of material misstatement.

- The organization to define the desired behaviours that characterize the entity's desired culture and demonstrates a commitment to the entity's core values.
- E.g. we often come across terms like code of conduct, whistleblower mechanism, vision and mission statements etc. These are means to enforce the culture and core values of an organization.
- The organization to design practices in such a manner that they attract, develop and retain capable individuals. E.g. Deciding the recruitment sources – open market, campus interviews, recruitment agencies; Designing tax friendly compensation structure for employees, encouraging eligible employees to get professional certifications relevant to their job profile/ career advancement etc.

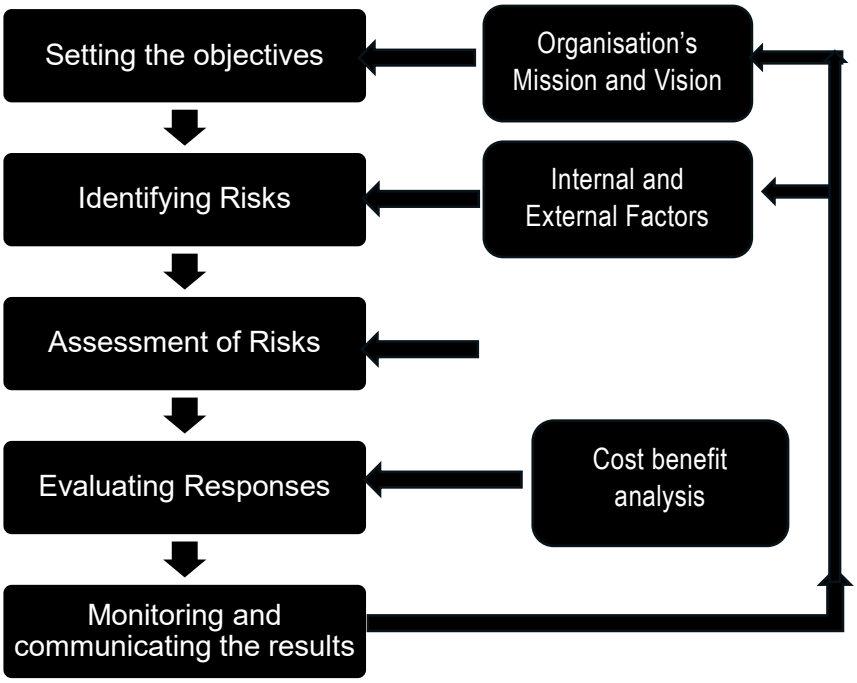
> **Governance**
>
> Governance refers to the framework of relationships among the organisation, its Board, management and other stakeholders, through which organisational objectives are established, achieved and monitored. It encompasses compliance with internal policies and procedures, as well as applicable laws and regulations.

All these aspects are related to setting governance practices in an organisation.

Many of the corporate failures have happened due to poor risk management and governance practices. The objective of Risk Management is to identify the risks attributable to such failures and establish relevant controls to minimise the potential risks and encash the opportunities with calculated risks. Such approach requires appropriate risk management practices and adequate performance reporting measures. Governance practices in the organisation lays down the internal controls, reporting and monitoring structures. Thus, the Risk Management and Corporate Governance are thickly connected to each other.

Risk Management Process

3.4 As the definition suggests, the Risk Management process identifies, assess, manages and controls the events that would potentially create an obstacle in achieving organizational objectives. The Risk Management Process may be narrated in the following way:



Risk Assessment

3.5 Risk assessment has two important aspects namely :

1. Identifying risk

2. Assessing risk.

Risk Identification

Risk identification is a set of activities that detect, describe and list all potential risks to operations and processes that could negatively impact business outcomes in terms of performance, quality, damage, loss, or reputation.

Internal auditors should identify events that may give rise to risks across the organization. Various methods that could be used for performing risk identification include:

(a) **Perform thorough Documentation Reviews:** internal auditor should thoroughly analyze relevant documents, policies and procedures collected during his understanding to identify potential gaps or

inconsistencies in risk management practices. Documenting review notes will help the internal auditor not to miss any critical information.

(b) **Interviews, Surveys, Questionnaires:** Interviews are crucial for gathering insights and information from key stakeholders. Internal auditors should prepare targeted questions, actively listen to responses and probe for underlying details to gain a deeper understanding of risks and control weaknesses. Internal auditors should interview key stakeholders such leadership team, board members, audit committee members, statutory auditors, consultants. Additionally, risk surveys or questionnaire are a highly cost-effective way to identify and quantify risks by gathering information, perceptions and insight from managers across an organization

(c) **Industry Risks:** Develop specific understanding of the risks and challenges faced by the industry in which the organization operates. To do this internal auditor can refer to and study various industry specific reports that deliberate risks and changes, Management Discussion and Analysis (MDA) section from annual reports of other listed organizations operating in the same industry, interviews with industry leaders. Internal auditors should also develop an understanding of industry best practices during this process.

(d) **Data Analytics:** Leveraging data analytics dashboards can help internal auditor uncover hidden patterns and trends in historical data and enhance risk assessment process. By leveraging the power of data, internal auditor can make more informed decisions and prioritize audit activities based on concrete evidence.

(e) **Review:** Reviewing past reports from various lines of control on audits, assessments and investigation can provide insights on the area/ processes that are more risk prone or do not have history of good governance and may need more attention.

(f) **Enterprise Risk Management Program:** If a strong risk management process exists in the organization, its workings, findings and suggestions would be reviewed and considered by the internal auditors as part of their planning process.

(g) **Brainstorming:** Internal auditors can conduct brainstorming sessions by bringing together team members to come up with as many risks as possible. Focusing on events that impact objectives is usually the

easiest way to brainstorm risks facing an organization. Brainstorming capitalizes on the team's diversity of specialization, understanding and experiences.

(h) **Review of MIS/ KPIs etc.** Achievement or non-achievement of desired business performance or Key Performance Indicators may provide a risk insight to the internal auditors. E.g. Deteriorating performance of a specific plant may trigger an insight towards review of viability measures undertaken by the organization, in case plant shut down is to be announced, internal auditors can provide consulting services like identifying contracts which will have to be terminated along with early termination penalties; if any.

While applying one or more methods of risk identification, the internal auditors should keep in mind and apply various concepts mentioned in above.

Top-down Vs Bottom-up approach

There are primarily two approaches for risk identification:

- Top-down; and
- Bottom-up.

Top-down approach is a macro level analysis that looks at high-level risks that are common across most auditable units. It helps in having a holistic view of the risks. This would require a high-level understanding of the organization, interactions with C-suite officials, Risk Management and Audit Committee member interactions.

A bottom-up approach is the opposite and is a micro level analysis that looks at risks to the specific line of business or entity or a process or a transaction. This would include interactions with the middle level management, heads of departments etc.

Internal auditors should make use of both the approaches as appropriate. It helps in capturing the intricacies of process/ transaction level risks which might turn out to be big risk or financial misstatements surprises if not controlled.

Internal auditors need to be mindful of the multifaceted nature of risks while identifying them. No single risk inventory exists for every organization; risks vary by organization and change over time. Revisiting changes in the

significant risk scenarios before every audit visit and accordingly suitably modifying the audit assignment strategy is desirable.

Risk Categories

3.6 Internal auditors should consider the following broad categories of risk to identify organizational risks:

- **Operational Risks** - Operational risk is the risk of loss due to ineffective or failed internal processes, people, systems, or external events which can disrupt the flow of business operations. These operational losses can be directly or indirectly financial.
- **Financial Risks** - These are risks that arise from an organization's financial operations and management. Examples include credit risk, market risk, interest rate risk, currency risk and liquidity risk.
- **Compliance Risks** - Specifically, compliance risk is the threat posed to a company's financial, organizational, or reputational standing resulting from violations of laws, regulations, code of conduct, or organizational standards of practice. Compliance risk could have potential exposure in terms of legal penalties, financial forfeiture and material/ reputational loss.
- **Strategic Risks** - If not managed properly, these risks have the greatest potential to affect the organization's ability to achieve its goal.
- **Technology Risks** – Technology supports business processes and is often integral to controlling processes. With increasing automation of internal control processes, deficiencies in underlying technologies may affect the organization's operations and business objectives significantly. IT risk can be further sub-categorized into infrastructure, operations and applications.
- **Third Party Risks** – Third-party risk is the likelihood that organization will experience an adverse event (e.g., data breach, operational disruption, reputational damage) when organization chooses to outsource certain services or use software built by third parties to accomplish certain tasks.
- **Environmental, Social and Governance (ESG) Risks** - Internal auditors should evaluate organization's ESG efforts, particularly alignment with stakeholder expectations (investors, customers,

employees, business partners, public) and legal requirements. In organizations that lack ESG criteria and reporting, the internal audit activity has an opportunity to help the organization increase its ESG awareness.

- **Fraud Risks** - Internal auditors also must assess and include fraud risks as part of each assurance engagement.

Internal auditors should understand and appreciate events that may generate risks like those list in the following table e.g.

Operational	Financial	Technology	Regulatory	Personnel	Material
Critical equipment failures	Theft or misuse of funds	Loss of internet	Contract violations	Attrition	Loss of trust by stakeholders
Material shortages	Liquidity crunch	Virus attacks	Non-compliance with legislation	Lack of required skills	Negative media publicity
Unavailability of manpower	Suboptimum use of available funds	Hardware failures	Delays in compliance	Integrity issues	Inability to meet commitments
Utility failures (electricity, water)	Inadequate expansion capital	Data unavailability		Increase in manpower costs	Frauds
Supply chain constraints	Currency fluctuations	Communication network loss		Inadequate succession	
Unavailability of workspace	Interest rate fluctuations	Internal network failure		Employee mishaps	
		Server failure			
		Phishing/ hacking attacks			

Within each broad category, internal auditors should consider internal and external sources of risk, which generates an extensive list. Internal auditors will need to assess those risks to narrow the list and prioritize them.

Risk Assessment Process

3.7 Standard on Internal Audit (SIA) 220, "Internal Audit Planning," requires that the internal auditor shall undertake an independent risk assessment of all the Auditable Units identified in the Audit Universe and align this with the risk assessment conducted by the management and the statutory auditor. This is required to prioritize and focus audit work on high-risk areas, with due attention to matters of importance, complexity and sensitivity. The internal auditor may also plan to undertake a dedicated audit of the company's Risk Management Framework and processes, as a separate review or assignment.

During the risk assessment process, internal auditor reviews both the likelihood and potential impact of various risks to the organization that have been identified by the Risk Management team or the management. In case the Risk Management team or management has not done that, then the Internal Audit would perform this exercise by himself in consultation with the management. The risk assessment process enables internal auditors to understand the relative significance of various risks identified.

Impact refers to the effect on an organization's performance if risk event occurs while likelihood refers to probability of the risk to materialize. Risk may differ in impact/s as some may have insignificant impact while the other may have catastrophic impact on the organization. Risks may also vary in their likelihood as some risks may be extremely unlikely and others could be almost certain. Hence to compare and prioritize risks it becomes important to rate them on impact and likelihood and get common score that can be benchmarked.

Determining Risk Impact

Impact of the risk can be evaluated using various risk factors and can be categorized into logical categories such as financial, operation, legal, strategic and reputational. A single risk could have impact on multiple categories E.g. breakdown on the plant could have financial, reputational, contractual impact in additional to operational impact.

While various models like 3X3, 5X5, 7X7 or 10X10 are used in the industry; generally, impact is largely rated on the scale of 1 to 5. For each category of impact, it will be important to clearly define parameters that will determine the rating. E.g., for financial impact it will be good to define value range for

each rating based on materiality of the organization. Some illustrative methods to determine impact are given below:

Risk Impact	Score	Financial	Operational	Legal and Compliance	Strategic	Reputational
	Sr. No.	Impact on revenue, cost or profitability	Impact on manufacturing or business process that results in a loss of productivity, quality or timely delivery	Impact in terms of regulatory fines, breach of customer contracts, lawsuits, or criminal charges, restriction on doing business	Impact on business strategic objective, long term growth, transformation	Negative media attention, customer dissatisfaction, relationship damaging impact with various stakeholders
Insignificant	1					
Minor	2					
Medium	3					
High	4					
Catastrophic	5					

Determining Risk Likelihood/ Possibility

The likelihood of the risk can be evaluated considering various risk factors using probability and time horizon of occurrence. Some illustrative methods to determine rate likelihood are mentioned below:

Risk Likelihood	Score	Description	Probability of event, risk materializing	Time Horizon – risk, event expect to occur with in
Very Likely	5	Very high probability that risk will materialize, almost certain or expected to occur.	>80%	1 year
Likely	4	Good probability that risk will materialize.	60%-80%	1-2 years
Moderate	3	Moderate probability that risk will materialize.	40%-60%	2-5 years
Unlikely	2	Low probability, remote possibility that risk will materialize	20%-40%	5-10 years
Rare	1	Very low probability that risk will materialize, extremely unlikely, almost nil	<20%	Beyond 10 years

Impact and likelihood are usually rated between 1 and 5. Risk scores can then be calculated by multiplying the two values together, giving a maximum possible score of 25. The risk along with the scores can provide risk heat map for the organization.

Refer Annexure 2 for conceptual models on Risk Management depicted by various professional bodies and risk heat map.

Para 6 of SIA 150 mentions that:

- Unless specially excluded from the audit approach, the Internal Auditor shall plan and conduct risk based internal audits. This requires the application of risk management concepts to ensure that the audits are prioritised in areas of urgency and importance, appropriate resources are allocated effectively where needed most, audit procedures are designed to give due attention to important matters and issues identified and reported are significant in nature.

- The nature and extent of audit procedures to be conducted in risk management is dependent on the maturity of the risk management processes and the framework in place. Where management has implemented a risk management framework, the Internal Auditor shall plan and perform audit procedures to evaluate the design, implementation and operating effectiveness of the organisation's risk management framework to provide independent assurance to management and those charged with governance
- Where no formal risk management framework exists, the Internal Auditor shall design and conduct audit procedures with a view to highlight any exposures arising from weak or absent risk management activities, make recommendations to implement and strengthen related processes and thereby improve risk management and mitigation.

Relationship between Risk Management and Internal Auditor

3.8 Where the organisation has a separate Risk Management function in the organisation than it is expected that the Internal Audit closely works with the Risk Management department. Internal Audit should leverage the work performed by the Risk Management department and evaluate the adequacy thereof. By leveraging the work of RM, Internal Audit can:

- Optimize its time over risk assessment exercise.
- Better relate its scope elements with the risks identified.
- Understand which other areas can be scoped in for internal audit projects.
- Always demonstrate that the internal audit is performed considering the risks which are most relevant to the business and not on the trivial scope areas.

Above elements help an Internal Audit function to successfully implement RBIA.

Role of Internal Audit in Risk Management

3.9 The Internal Auditor's job depends largely on how well Organisations' Risk management framework is defined. In case, there is no framework exists, Internal Auditor shall:

- modify the audit approach accordingly,
- undertake appropriate risk assessment across all major functions/ departments, with a view to highlighting exposure arising from absence of risk management activities.

The Internal Auditor shall review the risk management system and processes in place to evaluate whether they are operating in an effective and efficient manner and help to ensure full compliance. Any shortcoming highlighted shall result in recommendations for improvement and suggestions on how to make the risk management framework more efficient and effective in line with stated objectives.

Thus, although the Internal Audit and Risk Management work closely with each other, by exchanging their work outcomes with each other; it is expected that the Internal Audit maintains his independence appropriately. Internal Audit should consider the key risks identified by the Risk Management during his Internal Audit planning and execution of RBIA; he should also share his findings with the Risk Management which would enhance the overall Risk Management practices in the organisation.

In relation to the Role of Internal Auditor in the Risk Management Process, below are Possibilities of Assurance and Consulting Engagements:

- Assurance
    - Review of management of key risks – by assessing Risk Management activity as part of its overall assurance role
    - Evaluate reporting of key risks - by assessing the quality of reporting of key risks against established Risk Management frameworks (E.g. COSO Enterprise Risk Management)
    - Provide assurance that the risks are adequately evaluated - by assessing the entire risk evaluation process followed by the management

- Provide assurance on the Risk Management Process – by assessing the operating effectiveness of the Risk Management process

Execution of Engagements Relating to Risk Management Reviews by the Internal Auditors

- It is important to note that all basic principles of conducting an internal audit activity are equally applicable to these reviews. E.g. Engagement planning, Risk Assessment, Engagement Execution and Reporting are very well applicable to these types of reviews as well. However, there are few differences:
  - Underlying review context is at entity level instead of a process or transaction level.
  - Since the topic of Risk Management is little abstract (i.e. difficult to articulate compared to articulating routine business processes and its context varies organization to organization) and the auditees involved are senior management and board/ audit committee members, usually these engagements are conducted by senior experienced internal auditors.
  - The nature of Risk Management review procedures are largely driven by interviews, going through records, risk registers etc. Routine testing mechanisms like process walkthrough, sampling etc. may not be relevant in these types of reviews.
  - The outcome of these reviews has organization-wide implication and most of the times involve highlighting future implications of risks which require consideration in designing the business strategies.
  - Periodicity of these reviews may not be too frequent as compared to routine internal audit areas. It could be annually or bi-annually or even more considering the organization's context and risk management function's maturity.
  - It is important to note that these days many automated/ web based risk management solutions are available.

Therefore, an internal auditor might require an assistance from the system expert in evaluating such solutions for their effectiveness.

- Consulting
    - Facilitate identification and evaluation of risks - through structured discussions and brainstorming sessions with the management.
    - Coach management in risk response – by helping management in understanding various types of responses and evaluations thereof.
    - Coordinate Risk Management activities – by interacting with other teams in the organization.
    - Consolidate reporting on risks – by bringing them under a well structured reporting format.
    - Maintain and develop Risk Management Framework – by keeping the framework operational in absence of the risk manager.
    - Advocate establishment of Risk Management practices – by promoting the need for enhanced risk maturity in the organisation and its continuity and to achieve the next level of risk maturity (refer Annexure 1 on Risk Maturity Table).
    - Develop Risk Management strategy for the Board – by assisting the board in providing relevant inputs for the new Risk Management strategy based on his experience about the organization and its nuances.

  Subject to inherent safeguards to be applied w.r.t. independence and objectivity.

Do not Assume Risk Management Role

3.10 There are certain activities which the Internal Auditor should never perform by which there will be a potential conflict in discharging his duties as IA. The conflict could arise from self-review threat i.e. reviewing own work, loss of objectivity and independence. They are as under:

- **Setting Risk Appetite.** This task is of the management and the Board. Internal Auditor should merely assess whether the identified risks

overshoot the defined risk appetite and the related controls keep the risks well below the appetite threshold.

- **Imposing Risk Management** Processes on the management. The Risk Management function is the primary responsibility of the management and the Board and the Internal Audit is not in a position to impose it on either of them.
- **Reporting** on risks on behalf of the management. Internal Auditor is supposed to review the Risk Management practices and provide assurance whether the intended control framework is operating effectively and efficiently and significant risks have been identified and managed by the management. Providing appropriate response in the responsibility of the management and board and not of the Internal Auditor.
- **Taking decisions** on risk responses. Since the Risk Management is the primary responsibility of the management and board, Internal Auditor should not get involved in taking decisions on the risk response.
- **Implementing** risk responses on management's behalf as it would result in getting involved in the execution and in turn lead to conflict of interest.
- **Assuming Accountability of Risk Management**. Risk Management is the primary responsibility of the management and board and it is expected that they assume such accountability.

Therefore, Internal auditing can provide consulting services so long as it has no role in actually managing risks – which is the management's responsibility. It is necessary that the nature of internal auditor's responsibilities are documented in the internal audit charter and approved by the audit committee or board (i.e. the reporting authority) as the case may be to have an adequate safeguard to avoid possible conflict. Where Internal Auditor has been involved in any activity of Risk Management, as approved by the reporting authority, it is advisable that assurance of that area should be obtained from a third party.

Value Addition by Internal Audit function

3.11 Internal auditing activity provides value to the organization in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the risk management and internal control framework is operating effectively.

While doing so the Internal Auditor evaluates the adequacy of risk management and effectiveness and efficiency of the adopted control measures related to the following key risks:

- Strategic Risks
- Operational Risks
- Regulatory Risks
- Financial Risks

While evaluating the already identified risks, the Internal Auditor also evaluates the changing risk landscape and educates the management and board accordingly. By providing various consulting services, as narrated in the prior section, the Internal Auditor plays a very key role in the Enterprise Risk Management activity; especially where the dedicated Risk Management Function is not available.

The consulting activities provide internal audit with the greatest opportunity to add value to the business processes. As such, these consulting activities represent the majority of the roles Internal Auditor can assume in an effort to speed up the process of implementation of risk assessment methodology into the corporate governance framework.

Internal auditors generally have good insight in the organisation's activities and the significant risks it faces. They also have access to large data and board room discussions wherein great insight of business can be captured by them. Their knowledge of overall risk landscape of the global scenario and more particularly relevant to industry their organisation pertains to, make them a valuable resource in the Risk Management activity.

Chapter 4

Building a Risk Management Internal Audit Universe and Internal Audit Planning

Introduction

4.1 After understanding the important aspects of Risk Management, the next step is to comprehend how RBIA is put into reality. The first step is to understand how to build a comprehensive risk based internal audit universe and internal audit plan.

This enables Internal Audit function to align its internal audit work in line with the organization's biggest challenges/ priorities. In a way, the internal audit plan becomes dynamic considering the business dynamics. Therefore, risk-based approach allows audit teams to customize their audit activities to match the risk levels involved in the processes and controls that they are examining rather than prescribing specific requirements and scopes.

> A RBIA plan seeks to address critical risks first while a compliance-based audit seeks to evaluate an organization's adherence to a set of compliance criteria and process-based audit covers review of end-to-end activities without giving much importance to the risks' priorities therein.

Traditionally, internal audit has embraced a compliance/ controls-based approach that inspects and verifies that the operational, financial and compliance controls are operating according to an established set of criteria. Increasingly, internal auditors are turning to risk-based approach, driven by a more forward-looking perspective aimed at assisting management in addressing potential risks that could prevent an organization from achieving its objectives.

Developing a comprehensive risk-based audit universe is a crucial step in ensuring the effectiveness of an organization's internal audit function. It involves identifying and prioritizing the key areas of risk within the organization basis which internal audits are planned and executed. It also enables to align and focus its limited resources to produce insightful,

proactive and future-focused assurance and advice on the organization's most pressing issues.

Ensuring internal audit priorities are risk-based requires advanced planning. Ideally, the Chief Internal Audit or an equivalent senior level executive is responsible for developing a plan of internal audit engagements supported by experienced internal audit managers and internal audit staff. Nevertheless, the staffing and their designations would differ from organisation to organisation based on its size.

No single approach fits all organizations and the approach needs to be customized based on the nature of business, structure of organization, resources available, expectations of the stakeholders, the maturity of Risk and Control processes and Enterprise Risk Management. Typical stakeholders for internal audit include the leadership team (i.e. C-suite), the Board, Audit Committee and statutory auditors.

To develop an effective audit universe, it is important to first understand the organization's objectives and strategies. This will help identify areas that are critical to achieving these objectives and where risks may arise. E.g. If the organization's objective is to become leader in the manufacturing of auto components, then the internal audit universe should have its reflection covering associated areas like review of market share assessment, product defects, innovation activities, etc.

As a next step, a comprehensive risk assessment (if not already performed) should be conducted to identify potential risks across all areas of the organization. This can be done through interviews with key stakeholders, reviewing past audits and incidents and analyzing industry trends.

Once risks have been identified, they should be prioritized based on their likelihood/possibility and potential risk impact on the organization. This will help to determine which areas require more frequent or in-depth auditing.

Finally, it is important to regularly review and update the audit universe as new risks emerge or organizational objectives change. By following these steps, organizations can develop a robust audit universe that effectively addresses their key risks and supports their overall objectives. This approach is observed where the organisation does not have a well-laid Risk Management function.

Each of these aspects are dealt with in details in the following paragraphs.

Leveraging Entity's Risk Management in the RBIA

4.2 Organizations that have implemented Enterprise Risk Management may have created a comprehensive risk register (also known as a risk inventory or risk universe). Internal auditors may use this information as one of the inputs into risk based internal audit planning. However, to ensure independence and objectivity, internal auditors should do their own work to validate that all key risks have been identified and that the relative significance of risks is reflected accurately.

Para 6 of SIA 150 mentions that:

- Where management has implemented a risk management framework, the Internal Auditor shall plan and perform audit procedures to evaluate the design, implementation and operating effectiveness of the organisation's risk management framework to provide independent objective assurance to management and those charged with governance.

Understand the Organization

4.3 To develop risk-based audit universe the internal audit team should identify and understand not just high-level organizational objectives and strategies, but also specific business objectives and the strategies used to achieve them. Internal auditors will not be able to assess risks effectively if the organizational objectives are not clear. Organizations may categorize business objectives in logical categories such as strategic, operational, reporting and compliance.

While understanding the organization, it is important to develop the understanding about the following:

- The activities undertaken by an organization, lines of business
- Organization's geographical reach
- Macroeconomics of the industry, market sector volatility and challenges
- Positioning of the organization
- Quantum of organizational change
- Regulatory requirements governing the organization
- Organization's risk appetite
- Organization culture and tone at the top
- Risk and assurance requirements of key internal and external stakeholders.
- Various accounting and operating software/ platforms used; reliance placed on automations
- Engagement with various third parties/ outsourcing of business activities
- Subsidiaries and joint ventures with the organization
- Information about peers

Standard on Internal Audit (SIA) 220, "Internal Audit Planning," requires that the Internal Auditor shall gather all the information required to fully understand the entity's business environment, the risks it faces and its operational challenges. A key element of planning involves extensive discussion and deliberation with all stakeholders, including executive management, risk owners, process owners, statutory auditors etc. Their inputs are critical in understanding the intricacies of each assignment under consideration, in identification of important matters of relevance and to align stakeholder expectations with audit objectives.

Conduct Comprehensive Risk Assessment

4.4 An independent risk assessment by Internal Audit is typically required in the absence of a Enterprise Risk Management (ERM) or Risk Management (RM) function. Under such conditions, Internal Audit must independently identify, assess, and prioritize organizational risks to formulate an effective risk-based audit plan.

Where a mature and independent ERM or RM function exists, Internal Audit should rely on the enterprise risk assessment as a primary input, supplementing it through selective validation, challenge, and refinement to ensure completeness and reliability, while avoiding unnecessary duplication and maintaining audit independence.

Build Risk Based Audit Universe

4.5 An audit universe is a collection of potential audit areas/ activities to be performed by the internal audit function. It is made up of auditable entities, processes, systems and activities. An audit universe supports the development of the internal audit plan and help to identify appropriate internal audit coverage that the Chief Internal Auditor can then prioritize.

Standard on Internal Audit (SIA) 220, "Internal Audit Planning," defines audit universe as the complete identification of all the Auditable Units (locations, functions, business units, legal entities, including third parties where relevant).

Depending on the scale and complexity of the organization, the list of audit areas can run into several hundreds. The internal auditor needs to maintain right balance between too many and too few audit areas basis organization's hierarchy, spread, scale and complexity.

Key documents that can be referred to for identifying objectives, strategies, and structure of the organization:

- Vision Mission statements
- Management discussion and analysis (MD&A)
- Lines of Control working in the organization
- Organization chart
- Short-term and long-term strategic business plans

- Accounting policies and principles adopted
- Operating policies of the organization including process maps
- Annual reports and public/regulatory filings
- Organization level risk register (risk universe)
- Minutes of the key meeting with Board and Audit Committee
- Previous reports of audits and assessments from various assurance providers (second line functions, internal and external auditors)
- Substantiated investigation reports
- Actions taken in past against any unwarranted incidences
- Audit Charter
- Key legal contracts
- Financial statements and related materiality levels
- Industry specific reports, articles

The above list in indicative and not exhaustive. It may very as per each organization's context.

Risk based audit universe prioritizes potential audit areas basis of assessment of likelihood and impact of risks involved.

It is generally not mandatory to maintain risk-based audit universe; however, some organizations may have regulatory requirements that necessitate an audit universe to demonstrate completeness of coverage (e.g. banking sector and NBFCs). Hence where it is not mandatory to maintain risk-based audit universe it is a decision to be made by Chief Internal Auditor considering the advantages of having risk-based audit universe.

Advantages of having risk-based audit universe include:

- Help to in objectively determining the audit coverage of key businesses or functions to be presented to various stakeholders including the Audit Committee.
- Help to improve knowledge of the organization beyond risks and controls to various business strategies, industry specific knowledge therefore, improving the commercial awareness.

- Help to determine internal audit future headcount and skillset requirements including possible hiring, or co-sourcing to obtain a skill set.
- Help the organization achieve its objectives more efficiently or effectively by reviewing critical processes.
- Providing insight and comfort to the Audit Committee about adequate coverage of the internal audit activity.

Internal audit's decision to create an internal audit universe is often based on their independent view of the risk maturity within organization. Internal audit is more likely to create an internal audit universe if they assess organizational risk maturity to be in the initial stages of risk maturity such as Risk naïve, Risk-aware, or Risk defined (Refer Annexure 1 – Risk Maturity Table)

Audit Universe Categorization, Segments and Perspectives

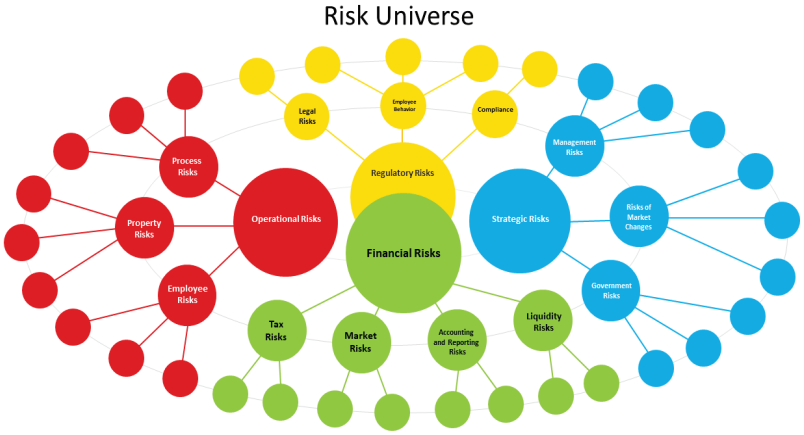
4.6 Risk based internal audit universe is a bigger canvass and internal auditor may not do justice unless its cut into logical sections.

Common categorizations of the Audit Universe

- Departments – various functions in the organization e.g. project, plant, purchase, sales, HR, compliance,
- Processes – procurement to payments, order to cash, production to inventory, hire to retire, treasury, asset management, health safety and environment, compliance
- Line of business or business unit depending on the organization structure
- Location - geographical location, headquarters, regional offices, branches
- Operational programs
- Strategic objective alignment - operational, financial, strategic and compliance

Note: in large organizations, the above categorizations may not operate in a linear way and may require combining more than one category. E.g. Some

areas will be covered by geography and some will be covered by departments. Centralized functions would not need categorization like geography or department e.g. Finance and Accounts may be covered at corporate office. Even it can include thematic audit areas which are not specific to a business process like Auditing “work from home facilities”.



There is no single best way to segment an audit universe. Each organization needs to determine what works best for it. A retail organization may, for instance, want to have separate auditable areas for each of their branches or outlets to enable risk assessment and coverage of operations where local managers are mitigating risks at the front line on a day-to-day basis. Refer. HEAT map given in Annexure 2.

Some organizations, in particular large international ones, may find it useful to leverage multiple perspectives in their audit universe to enable views through more than a single lens (a multi-dimensional audit universe).

Ensuring Completeness of the Internal Audit Universe

4.7 It is important for the Internal auditors to ensure and convey the comprehensiveness of the audit universe to the stakeholders such as leadership team, audit committees, external auditors and regulators. In the real sense, the ability to convey the comprehensive audit universe is the starting point of giving objective and independent assurance. This can be done in couple of ways:

(a) **Mapping to the Strategy Documents**: The audit plan may be mapped to various management initiatives, existing or proposed, emerging from strategies, Board presentations, Board sub-committees initiatives, departmental strategy literature etc.

(b) **Mapping to Organisation Chart:** Broadly reconcile the auditable areas within the internal audit universe to organization charts and to socialize the auditable entity structure with the Audit Committee, executive management and external audit.

(c) **Mapping to Trial Balance:** Reconcile the auditable entities to the trial balance at an appropriate granularity of revenue and cost centers. This is useful but potentially time-consuming exercise.

For illustrative Risk Based Audit Universe format Refer Annexure 3.

Preparing Risk Based Internal Audit Plan

4.8 Due to the large number of risks and possible audit areas in the audit universe, internal auditor should determine what needs to be prioritized and audited from within the developed risk-based audit universe.

As per Standard on Internal Audit (SIA) 220, "Internal Audit Planning," conducting the Overall Internal Audit Planning involves the following key elements:

- Ensure that an Internal Audit plan is in line with the objectives of the internal audit function, as per the internal audit charter/ manual of the entity and also in line with the overall objectives of the organisation.
- Align the organisation's risk assessment with the effectiveness of the risk mitigation steps implemented through internal controls.
- Confirm and agree with those charged with governance the broad scope, methodology and depth of coverage of the internal audit work to be undertaken in the defined time-period.

Ensure that overall resources are adequate, skilled and deployed with focus in areas of importance, complexity and sensitivity.

Internal auditor can prepare audit plan for a particular time period (usually a year) considering various parameters such as:

- **Risk Factors** – Internal auditor can use various risk factors to review the importance of each element of the audit universe to determine the priority to be attached to each auditable object.

- **Risk Appetite** – Level of risk that an organization is willing to accept in pursuit of its objectives.
- **Assurance Requirement** – Legal requirements governing the organization around internal audit.
- **Stakeholder Expectations** – Expectations of key stakeholder should be considered here such as leadership team, audit committee, statutory auditors, industry best practices.
- **Resources Available** – In the competitive world today every function has limited resources and the internal auditors too will need to determine the amount of work that can be performed with available resources such as team, cost budget, tools available, etc.

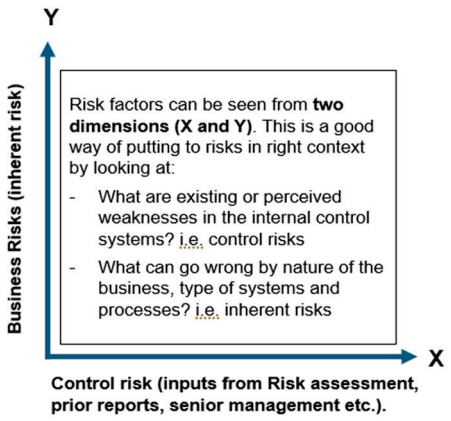
Various other risk factors to be considered while prioritizing the risks include:

- Financial materiality
- Complexity of operations
- Control environment - Strength of defined controls, policies, authority matrixes
- Impact on the strategic objectives
- Level of activity - frequency, volume, number of transactions.
- Manual Vs automated Vs IT enabled controls
- Statutory/ regulatory compliance requirements
- Reputational impact
- Fraud potential
- Competency of the people involved and management
- Inherent risk
- Past performance
- Past audit findings, ratings, when last audited
- Recent changes to the process
- Third-party reliance

Many organizations follow a practice of designing “three-year audit plan” to be reviewed and suitably modified on an annual basis.

Internal auditors should select the risk factors that make the most sense for the organization in order to prioritize audit areas. It will be good to keep the number of risk factors to between 4 and 8. Too few risk factors will limit the effectiveness of the exercise and too many will increase the time it takes to and will not produce substantially better results.

It is desirable to include a mix of scheduled, surprise and survey or mystery types of audits in the internal audit plan. Especially in a typical bank set up, a branch is an auditable unit and its numbers could be numerous. In such a case quantum of surprise audits could be very high.



Ref. RBI Guidance Note on Risk Based Internal Audit

Internal auditors should record the justification for the selected audit areas in the audit plan. The justification for audit areas selected will help in providing reasonable assurance to various stakeholders about effectiveness of internal audit process. Standard on Internal Audit (SIA) 220, "Internal Audit Planning," requires that all key steps undertaken in the planning process shall be adequately documented to confirm their proper completion.

Ideally, annual internal audit plans should be prepared before the next year begins.

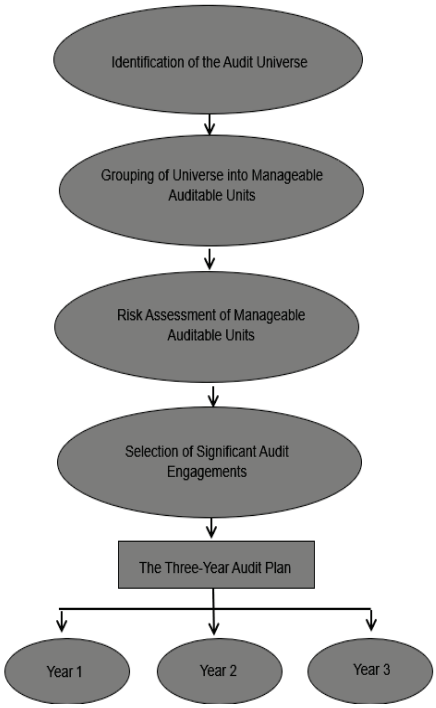
Standard on Internal Audit (SIA) 220, "Internal Audit Planning," requires that the audit universe and the overall internal audit plan shall be continuously monitored and modified as appropriate. Any significant modification to the plan shall be done only after consultation with those who approved the original plan. Such changes shall be formally documented, including reasons for the change and communicated to all impacted stakeholders.

Internal Audit Strategic Plan

4.9 The internal auditor should also document the internal audit strategic plan as well. It is an opportunity to present to management all the things that an internal audit function can do to help the organization to achieve its objectives. It can be a useful way of generating support.

Key elements of a strategic plan should be:

- Objectives and performance indicators for the Internal Audit function, linked as appropriate to the strategy for the organization
- Plan to address the areas of most significance over a period of years (cycles of coverage for different elements of the audit universe)
- The resources required and available to meet these needs. The impact of resource constraints on the ideal level of audit coverage
- Aspirational goals for what the Internal Audit function would like.



- Plans leverage work performed by other sources of assurance (e.g. internal controls, external audit)
- The approach for following up recommendations made
- Organizational constraints, if any.
- Assumptions made, if any.

As per Standard on Internal Audit (SIA) 220, "Internal Audit Planning," the overall internal audit plan shall be reviewed and approved by the highest governing body responsible for internal audits, normally, the Board of Directors, or the Audit Committee

Internal audit plans, and material changes thereto, should be approved by the audit committee or by those charged with governance (TCWG). The approvals should be documented in the form of minutes of the meeting and maintained in line document retention irements.

Standard on Internal Audit (SIA) 290, "Communication with Management and Those Charged with Governance," defines Those Charged with Governance (TCWG) as either an individual, or a body of individuals, or a separate legal entity with the responsibility for overseeing the strategic direction and accountability of the organization.

"Management" refers to persons(s) with executive responsibility to run the company's operations.

In the case of companies under Companies Act, 2013, it is a legal requirement for the Audit Committee or its Board of Directors to formulate the overall internal audit plan of the company Rule 13(2) of the Companies (Accounts) Rule 2014 provides as: "The Audit Committee of the company or the Board shall, in consultation with the Internal Auditor, formulate the scope, functioning, periodicity, and methodology for conducting the internal audit."

(Refer Annexure 4 for applicability of Audit Committee in India)

Stakeholder Feedback and Alignment

4.10 After the risk-based audit plan is prepared, the proposed plan should be shared with key stakeholders to solicit their feedback such as leadership team, audit committee members, statutory auditors etc. Adequate discussions should be held to understand concerns and efforts should be made to address them adequately as far possible and reasonable.

Stakeholders buy-in is critical to ensure success of the audit plan to maximize the benefits of the internal audit activity to the organization.

Communication of the Internal Audit Plan

4.11 After the risk-based audit plan is adjusted to the feedback received; the same should be formally communicated to for their inputs/ approvals as appropriate:

- Leadership team, audit committee, statutory audits

- Various process owners who will be part of these internal audit reviews
- Entire internal audit team
- Other lines of control

Standard on Internal Audit (SIA) 290, "Communication with Management and Those Charged with Governance" defines essential matters of communication with TCWG which includes Annual Internal Audit plan, covering the scope, timing, methodology of audit assignments to be undertaken, along with resources and budgets of the internal audit department.

Updating the Risk Universe

4.12 Risks are dynamic in nature and change over time. In addition, events that actually happen will generate new risks for the organization that were not there earlier (e.g., a major reduction in the budget). Internal auditor must therefore monitor significant events that occur during the year and the impact these may have on the audit plan.

Thus, the risk-based audit universe should be refreshed and updated at appropriate frequency, at least annually.

Assess Risks Continuously

4.13 Risk assessment is an ongoing process. To be agile and relevant, internal auditors need to continuously assess risks faced by the organization. Though formal risk assessment may be performed annually it will be good for internal auditors to connect with various stakeholders quarterly to assess risks. There could be event based unplanned change to the risks which are previously identified due to unusual business situation E.g. work from home scenario during COVID – 19 pandemic times which created new set of business and operational risks.

As part of continuous risk assessment, internal auditor should pay specific attention to:

- New or emerging risks
- Change in processes, tools, platforms, software
- Change in strategies
- Change in market conditions

- Disruptive technologies or global events
- New litigations, fine, penalties
- Change in team or leadership
- Changes in the regulatory requirements
- Inputs from those charged with governance (Senior management, board/ audit committee members)
- Change in the organizational control environment/ structures

4.14 The internal auditor should also review suggestions and recommendations on audit plan received from TCWG during the year/ period of audit plan executions and include them appropriately in the audit plan as and when received.

The Internal Audit should update the Internal Audit Plan and Communicate it is all concerned.

- The inputs collected in continuous risk assessment audit plan should be adjusted and updated for critical risks identified.
- Various stakeholders should be brough on board and be aligned with such changes.
- Formal communication of such changes along with rational for changes should be ensured.

Common Pitfalls in Risk Based Internal Audit Planning

4.15 Internal auditors should be aware and avoid following common pitfalls that will reduce the effectiveness of the risk based internal audit plan:

- **Lack of buy-in/ alignment with the leadership team and other stakeholders** – The risk assessment conducted by internal audit to prioritize audit areas should be discussed and aligned with the leadership team and other key stakeholders to ensure buy-in of the risk based internal audit plan from them. Internal auditor should consider the feedback received from these stakeholders and communicate back to them the changes made/ rational for the changes not made to the risk based internal audit universe/ plan based on their inputs. This goes a long way in building mutual respect. It is also important to decide about

the timing of auditing the areas where there is a change. i.e. to decide whether the area will be taken up in the current scope or the future scope.

- **Not updating risk-based internal audit universe or treating it as a one-time activity** – The audit universe or the risk-based audit plan needs to be agile. If the internal auditors fail to monitor, review and update them on the basis of various changes (discussed earlier) in the organizational circumstances then the risk-based audit plan may not remain relevant.
- **Not covering key risks over defined period under internal audit without valid justification** – Given the limited resources internal auditor may not be able to cover all audit areas in one year or a limited period. But the internal auditor should be able demonstrate to the stakeholder as to how significant risks have been covered over a reasonable period (say 2-3 years) to provide required assurance on control design and operations.
- **Setting Risk Appetite for the Organization** – Internal auditor should refrain from setting the risk appetite for the organization rather internal auditor should assess and comment on adequacy of the risk appetite. Risk Appetite is set by the Board and should align with strategic objectives that the organization wants to achieve. Strategic objectives and/or highly ambitious targets that are more difficult to reach would typically require a higher risk appetite.

Tips to Maximize Results of Risk-Based Audit Planning

4.16 With risk-based audit plan effectively implemented, internal auditor is well positioned to assess the effectiveness of risks mitigation measures and support the achievement of organizational goals. However, to maximize internal auditor should focus on further impact and drive sustainable improvements:

- **Track Progress and Measure Impact:** Regularly monitor the implementation of recommendations and track progress towards achieving risk management objectives.

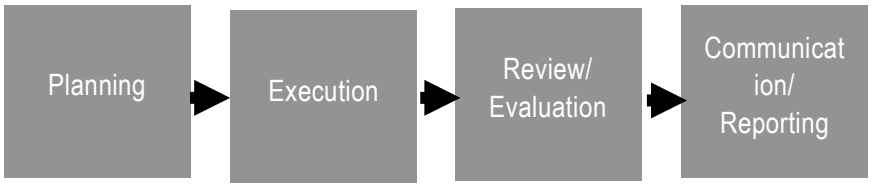
- **Quantify Benefits**: Assess the financial and non-financial benefits of risk management program, such as reduced costs, early warning signals of potential wrongdoing, improved efficiency and enhanced reputation.
- **Share Success Stories:** Showcase the positive impact of risk management program through success stories and case studies to build buy-in and encourage continued commitment.
- **Continuously Improve:** Regularly review and update risk-based audit plan based on new information, emerging risks and changing organizational priorities.
- **Promote Risk Awareness Training:** Educate employees at all levels about their roles and responsibilities in identifying, reporting and mitigating risks.
- **Encourage Open Communication:** Foster a culture where employees feel comfortable discussing risks and concerns without fear of reprisal.
- **Lead by Example:** Set the tone from the top by demonstrating a strong commitment to risk management principles and ethical behavior.
- **Recognize and Reward Risk-Aware Behavior:** Acknowledge and reward employees who identify and report risks effectively, further reinforcing the importance of risk awareness.
- **Embed Risk Management into Daily Operations:** Integrate risk management considerations into decision-making processes and daily workflows to ensure that it becomes an integral part of organization's DNA.

By prioritizing both maximizing results and building a culture of risk awareness, internal auditors can create a self-sustaining ecosystem where risk identification, assessment and mitigation become ingrained in organization's core values and practices.

Chapter 5

Executing Risk Based Internal Audit (RBIA)

Overall sequence of executing RBIA is as below:



Issuing Assurance Reports (SIA 320): Any internal audit assignment in which the internal auditor expresses an opinion on the outcome of the internal audit work to give an indication over the subject matter after comparing it with a pre-defined criteria renders it to be an assurance assignment. These are called an Internal Audit Assurance Assignment. SIA 120 para A4 refers to these as follows:

- Reasonable Assurance: Requires extensive procedures and evidence
- Limited Assurance: Involves limited procedures; expressed with appropriate disclosure of limitations. (Refer SIA 320 Para A3)

Pre-defined Criteria stipulate the manner in which an evaluation or measurement of the subject matter can be undertaken using an objective and consistent methodology and within the context of professional judgment. For e.g. an Internal Control Framework.

Internal Audit Assignment Planning

5.1 Once the Internal Audit plan is prepared and approved, internal auditor shall work on execution of the plan at the assignment level. This is achieved by detailing at each assignment level considering the scope and objectives. There may be a lag between the preparation of the Risk Based Internal Audit Plan and the Risk Based Internal Audit Assignments and/ or there may have been changes in the various Organization processes, practices and risks. This plan should have detailed note on:

- **Scope of Internal Audit:** Within area selected for Internal Audit during the year, Auditor shall define the aspects of the area to be covered under audit. Exclusions, if any, should be also identified/ stated. For example, if Payroll is selected for internal audit, then the following aspects can be considered for in scope:
    - Payroll processing (inhouse/ outsourced)
    - Hiring and onboarding
    - Termination
    - Annual increments and bonus/ incentive
    - Attendance and leave management
- **Risks identified during the walkthroughs and inputs from Managements:** Risks identified during the walkthrough help in elaborating the scope. Walkthroughs generally reveal the level of internal controls existing, proposed etc. For example, when talking to the Payroll Head about changes in the computer system in line with the recent changes to the payroll structures, internal auditor may note that the changes made to the computer system are not adequately tested. This creates a risk that the changes may not enable accurate and complete processing of the payroll. This may indicate performing specific testing of the payroll system.

  Previous Internal Audit observations/ other audit observations, their implementation status**;** any other audits-HO/ CO, Central Auditors, GST, Statutory, IFC audit observations, Fraud Investigations etc. can also be referred.
- **Testing approach (sample testing or analytical):** After due consideration of scope and mapping of controls with identified risks (to identify gaps, if any) testing approach can be defined. For example, if payroll processing is selected for audit, then analytical testing can give better result and coverage. This is always subject to availability of data in the electronic form, availability of required computer system programs for analysis and their hands on knowledge. On the other hand, if hiring is selected under scope, then sample testing can help better with verification of documents for the selected samples.
    - SIA 230, Internal Audit Evidence issued by the Internal Audit Standards Board provides guidance on sample size, sampling

approach, evaluation of sample results, reassessing sampling risk and documentation. Considering the availability of data and information in electronic form and the advanced technology and usage of data analytics methodology, the stakeholders' expectations have increased to cover the entire population under the review and reduce the usage of sample testing. Nevertheless, this would depend on the quality and state of data and maturity of the organisation.

- SIA 230, Internal Audit Evidence provides guidance on how the analytical procedures can be used in in planning, risk assessment and as substantive testing procedures.
- **Preliminary list of tests to be performed on the data:** Planning memo enlisting detailed tests to be performed, on the data received, accelerates the audit execution and better conduct

- **Information requirements (files and formats to be specified):** Next step in planning is to enlist the data required for audit. Population requirement for analytical testing and sample selection can vary in terms of formats. With the technology advancements, it is possible for internal auditors to have an access to required data and it can be easily obtained upfront before starting the audit.
- **Timelines:** Defining timelines is crucial in order to keep all stakeholders (audit team and process owners) on the same page in terms of information sharing deadlines and timely completion of the assignment.
- **Resource requirements and allocation of work:** Planning of resources in line with scope of audit is essential to conduct audit in an efficient manner. Number of areas scoped in, tests enlisted, data to be processed and timelines defined shall be analysed together to identify number of resources required, period for which each resource is to be engaged and qualifications/ skills of the resource to be deployed. E.g. in case of internal audit of suppliers' performance and relationships, an experienced staff shall perform the audit. This is because this assignment area is non-routine, cannot entirely be covered using transactions' testing. It requires interviewing skills, data analysis and its correlation with the other audit inputs, etc.

- **Audit tools and IT systems requirement:** If the transactions in the assigned audit area are voluminous, say, more than a million, then the audit in-charge will have to consider tools which would be required to obtain, understand and analyse such data and also availability of an internal expert who will work on this analysis. If the internal expert is not available, it is necessary to get external help considering the permissions from the auditee and legal safeguards in engaging such external expert. Also, such analysis requires a considerable time and therefore, allocating sufficient amount of time is necessary.
- **Define auditees:** It is important to identify and agree who will be auditees i.e. the various personnel with whom the Internal Auditors will discuss the Internal Audit Report and close the Internal Audit Assignment. The auditees may be Operations heads/ supervisors, Head of Department, Vice Presidents, Business heads, CFOs, COO or Board Committee and/ or the Board of Directors. The exact protocols to be followed should be known during the planning stage.

Internal Audit Assignment Execution

5.2 The Internal Audit assignment may be executed as follows:

- **Kick off Meeting**: A formal meeting to initiate audit is necessary to ensure all personnel are properly informed regarding the audit and of various aspects enlisted in planning stage above.
- **Incremental Walkthroughs**: A walkthrough involves tracing a transaction or process through its entire cycle to verify the design and effectiveness of internal controls. This procedure helps auditors understand how controls are applied in practice, identify gaps or weaknesses and ensure that controls align with documented procedures. Walkthroughs are essential for validating that processes operate as intended and for assessing the effectiveness of control activities.
    - Walkthroughs will consist of audit procedures to *test design* of the controls and process and its compliance by techniques such as observing, enquiring, systems/ process understating (including various IT systems), in-depth checking of sample transactions, reviewing monitoring controls etc.

- In walkthroughs Internal auditor should also test the *adequacy of the response to risks.* The audit procedures to test the internal controls would include verification, re-computation, reconciliation, negative testing, etc. prior to assessing whether the type of response, such as termination, treat, transfer or tolerate are adequate. Controls can be Manual, Automated, Mix, Preventive, Detective, Corrective, Financial, Operational, Application, ITGC, etc. (refer SIA 140, Internal Controls). These audit tests should confirm their existence, whether operated by appropriate personnel, whether they are resilient, i.e., will resist sabotage, reliable i.e. will achieve the control objective of mitigating the designated risks. Regulatory compliance risks may also require testing during walkthroughs.

- **Data Analysis:** This is a crucial process used to evaluate and interpret data to identify risks, trends and anomalies that could impact an organization's operations or financial statements It is important to note that the exceptions revealed out of data analysis, may not necessarily be the observations. There could be genuine business rationale and authorizations available for such exceptions. Hence, an auditor is required to do deeper scrutiny of such exceptions in order to decide if these are real problem issues. With an advancement in technology, choosing a right tool/ Artificial Intelligence (AI) based solution for data analysis/ RBIA execution becomes an important consideration.

Specimen case study for data analysis:

Scenario: XYZ Bank is a large bank having its branches all over India. It has got more than 15 million customers. Know Your Customer (KYC) information is stored in a separate KYC software which has interface with the XYZ Bank's core banking solution (CBS). There are 5 different documents collected for each customer as per the legal requirements and policies of the Bank. The Bank has its own internal audit and systems audit departments which work together in case of complex audits.

Internal Audit Objective: Verify completeness of KYC documents as on 31 Mar 20XX.

Internal Audit Challenge: Data to be analyzed is huge i.e. 15 million X 5 = around 75 million records. Some of these records will be in scanned form and some of these could be in digital form.

The volume of transactions compels an internal auditor to deploy tools which can handle such large records. Manual sampling will not be effective for the stated audit objective.

Approach: Noting the above internal audit challenge, Chief Internal Auditor consulted with the Systems Audit Head about possible ways in which the audit objective can be achieved. After deliberations, the following audit approach was adopted:

- Informing IT team about the 31 Mar 20XX cut off well in advance so that the data exchange between KYC software and CBS can be aligned.
- Data extraction strategy is decided considering the system resources that will be required to extract such huge data. It was decided to extract the data per region to ensure minimum load on the system and ensuring smooth operations of KYC software and CBS on an ongoing basis.
- Data extraction included:
    - Segregating the scanned data and data in electronic form
    - Using Optical character recognition (OCR) software for extracting key fields in scanned documents
    - Each OCR extraction output file to contain reference to unique customer number, document header and key field reference.
- All extracted information shall be stored on the Bank's private cloud which would only be accessible to the select members within Internal Audit and Systems Audit team.
- All data will be imported in the Bank's specialized Audit Tool by the Systems Audit
- Internal Audit team members will work with Systems Audit team member to decide the norms of completeness and exception.
- Systems Audit team member will then write the queries which will find necessary availability or non-availability of KYC documents per customer. Also, additional query is written to

identify duplicate KYC documents across all data. Audit team discussed with the bank's operations' staff about situations in which such duplication, if any, can happen.

(Refer Standard on Internal Audit (SIA) 220, Internal Audit Planning)

- **Continuous Discussions with Auditees**: All the audit observations/ queries, etc. during audit execution should be forthwith discussed with the respective auditees to ensure that there are no misunderstanding of the procedures, controls or facts and adequate transparency is maintained unless the circumstances warrant otherwise like in case of suspected fraud.

Audit Evidence (Refer SIA 230)

5.3 Audit evidence is the information used by the Internal Auditor in arriving at the conclusions on which the auditor's conclusion is based. Thus, internal auditor shall ensure that the evidence is sufficient and appropriate.

Evaluation of evidence involves:

- verifying the source (who has shared it, format in which it is shared, whether it is editable file),
- validity (whether in line with set policies),
- appropriateness
- relevance

Sufficiency refers to the quantity or quantum of evidence gathered while appropriateness relates to its quality or relevance and reliability.

Sufficiency can be determined considering the sample and control, e.g. if specific control says there is a need of only one level approval to enter into transaction, but the risk and amount involved is higher and authorisation matrix is silent, then senior level management's approval can be considered as sufficient.

It is important to note that there is a difference between mere including information received from an auditee "as it is" in the audit file and including it as an auditing work paper. An ideal work paper will include:

- Population, its source.
- Internal auditors' preliminary analysis/ checking to establish the relevance of the population to the testing objective.
- Actual audit work performed – sampling/ analytical procedures, etc.
- Conclusions drawn and cross reference to internal audit observations.

On the other hand, if any sample of "review type" of control is picked, (e.g. review of provision for bad and doubtful debts), then mere transaction/ calculation testing is not sufficient. An auditor will have to find:

- Who prepares such working.
- Whether the data is maintained manually or in the computerised environment or ERP system.
- Whether data extracted from computerised environment or ERP system requires an edit for making it ready for provision working.
- Whether there can be selective additions/ deletions and edits to such data by the preparer of provision calculation. If yes, who ensures that the edits are appropriate and authorized?
- Who reviews the assumptions to the working (e.g. cut-off of the data, data is pulled for all the locations, etc), parameters i.e. time period buckets used for classifying the receivables data, etc.

All the above and documentation of the review performed, issues noted during review and action taken to correct it, combined together will be appropriate audit evidence to conclude.

Audit evidence can be physical, documentary or analytical. In today's digital parlance, most of the evidence is in the electronic format. 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 objective of internal audit.

(Refer Standard on Internal Audit (SIA) 230, Internal Audit Evidence.)

Internal Audit Documentation (Refer SIA 250)

5.4 Each stage performed under internal audit assignment, shall be documented in order to support the final conclusion and submission of the report to the management and also for all future references.

Work not documented properly may lead to inappropriate conclusions by the reviewer of the documents and may give misleading information to the reader of the final report. Besides that, the Internal Audit would find it difficult to justify his conclusions and appropriateness/ adequacy of the work performed; it should be required later, in case of investigations, etc.

Documentation at various stages of internal audit are:

- **Planning:** Details of the entity, its business, industry, internal environment, areas which are prone to risks and basis chosen for selecting particular area for audit scope.
- **Data Requirements:** Documented list of requirements helps both parties (auditor and auditee) to be on same page in terms of information to be shared.
- **Evidence:** Evidence gathered during audit shall be kept together, sequentially in line with the risk and controls tested, to support the conclusion. Cross-referencing of audit evidence with the work scope (e.g. evidence for Risk1 control1 can be named as R1(file name) to easily locate the evidence while reviewing the testing workpaper), helps quick extraction of data.
- **Conclusion:** Either positive or negative, conclusion shall be documented (written down) against each audit performed (sample or analytical test) for easy summarisation and conclusion at overall audit plan level.

Based on the results of internal audit procedures, observations noted should be documented. Decision can then be made on which observations shall be carried to the draft report.

Important to Remember

Many times auditors try to complete the field work and then complete the audit documentation. Though it appears logical and sequential, this approach has its own limitations. Mainly, the audit documentation includes many things beyond the data supplied by the auditee. E.g. it includes

exception evaluation, facts corroboration, individual testing objectives and conclusions, management explanations, reasons for further analysis and so on.

With the advancement of technology, it is possible to document the work **on the same day**. Inherent benefits of concurrent documentation are:

- An auditor need not memorize the information gathered/ evaluated. Memorizing the information for a longer time is difficult.
- Understanding gained during the documentation gets automatically cross verified when an auditor starts putting it in a work paper since writing something as audit evidence puts moral obligation on the auditor to check genuineness of the audit inputs.
- Once the daily understanding is included in the work paper, then it is easier for an auditor to think clearly and freely for the stated audit objective. Therefore, the documentation process itself suggests few more audit considerations which could be relevant in finding internal control lapses/ enhancements.

(Refer Standard on Internal Audit (SIA) 250, Internal Audit Documentation)

Review and Supervision of Audit Assignments (Refer SIA 260)

5.5 Supervision refers to the oversight of the audit activities and the provision of overall guidance for the achievement of audit objectives. Supervision is an ongoing activity during the audit execution phase.

Review refers to the examination of audit plan and procedures, collection of audit evidence, conclusions drawn therefrom and documenting them into the working papers. This is usually done towards the end of the execution phase. However, supervision is recommended at three stages of audit assignment viz., start of the audit assignment, while the work is in progress and during closure of the assignment.

During review and supervision, the internal auditors may have to revisit the audit and resource plan and evaluate audit procedures.

Thus, while planning resource allocation, supervisory role also needs to be considered and assigned to a senior employee who can review the work

performed by the team and guide them in executing the audit, review of evidence, etc.

Refer Standard on Internal Audit (SIA) 260 , Review and Supervision of Audit Assignments/ Annexure 1 for "Indicative List of Review and Supervision Activities"

Communication with Management and Those Charged with Governance (Refer SIA 290)

5.6 The Internal Auditor is required to have an effective two-way communication with the management and Those Charged with Governance (TCWG), both while managing the internal audit function and while conducting an internal audit assignment. A continuous dialogue with management and TCWG, at various stages of the internal audit process, is essential to the achievement of internal audit objectives.

Explicit and timely communication helps an internal auditor to demonstrate his professional behaviour.

Communication with the management is throughout the assignment. Right from initial discussions, negotiation, scoping, signing off the engagement letters, audit plan communication, data requirements, queries, obtaining management responses, issuance of draft and final reports, presentations to senior management, audit committee and board of directors etc. – all these activities are nothing but different forms of communications.

Forms of Communication

- Though there are many forms of communication like verbal, written, gestural etc., an internal auditor is mainly concerned about the written and verbal communications.
- In good old days written communication (hand-written or printed) was the only mechanism to communicate with the management which would be acceptable in the court of law. This is still widely followed. However, with the technological advancement, new medium of communication has emerged i.e. electronic communication.
- Email is considered to be most efficient and commonly used mechanism for communication these days. Social media communications, though convenient and easy, are to be discouraged as it may be breach of communication protocols of the organization and generally not

considered as acceptable form of communication. Therefore, an internal auditor should avoid communication (especially the legal and confidential matters) through social media.

- With the COVID-19 pandemic, another form of communication gained a wide acceptance i.e. electronic meeting. These meetings are helpful as they offers virtual capabilities, removes all the logistical bottlenecks in arranging the physical meetings. There are many platforms available in the market that support virtual meetings.
- These electronic meetings allow presenting/ sharing of information like documents, presentations, images, sound files. Some platforms even allow recording facility so that the communication can be preserved/ reused as a reference for future purpose.
- While choosing the electronic meeting platform, internal auditors should ensure that the platform is from the reputed vendor, is secure from the possible threats like unauthorized interception, misuse, availability of data and more importantly, is in line with the organizational policies.
- Also, some entities prefer using their own secured cloud-based drives or portals for sharing of information. Internal auditor should have capability and understanding of these information sharing mechanisms so that overall audit efficiencies can be enhanced.
- Many times multiple version of the same data is stored on the computers/ laptops which may finally lead to the confusion about the uniqueness and authenticity of the data. To avoid this, internal auditor can establish a discipline of handling, accessing, storing, backing up this data. This could be simply achieved by way of putting a discipline over dedicating a specific drive (hard drive or cloud drive) for the particular work, deciding the naming conventions for folders, sub-folders, document version controls etc. considering the stage of work. Example:

M/s ABC & Co Chartered Accountants are undertaking an internal audit for a multinational manufacturing company (MNC). MNC has its own protocols of sharing the information through established cloud service providers. In this case M/s ABC & Co decides following approach in handling the information:

- Obtained, read, understood and signed off the obligations (including legal obligations) in handling the MNC data as set out in the MNC's data sharing policy.
- Identified the manager within the firm who will have primary access to the information.
- Manager then identified people working on MNC audit who are required to have access to MNC's data. Accordingly, their email ids are communicated to the MNC audit coordinators.
- Classified or sensitive data like payroll masters are kept accessible to the manager and above.
- Raw data received by M/s ABC & Co is shared in the folder "Received from MNC" with the subfolders assigned for audit areas.
- Audit work is stored in the folders containing audit area name, stage of completion (Draft/ work in progress etc.).
- Completed work is moved by the field staff into the folder "Ready for Review".
- Draft report, final report and all reviewed final work papers are stored in the folder "Client Reporting".
- Regular back-ups are taken to avoid any loss of data.

Timing of Communication

Timely communication helps in achieving internal audit effectiveness. Agreeing upon a schedule of communication in advance helps in avoiding understanding/ expectation gaps and unwanted surprises.

Following is one of the specimens of such communication agreed upon with the management by M/s ABC & Co. Chartered Accountants:

From: M/s ABC & Co Chartered Accountants

To: XXXX, MNC Co

Place, XXXXXXX

Subject: Communication of internal audit schedule

Dear Sirs,

Based on our discussion, we have prepared the following internal audit schedule. Request you to go through the same and approve so that we can commence our audit work.

Audit activity	Tentative Timelines
Reaching the audit location XXXX	1st Week of August 20XX
Process understanding and performing walkthroughs	1st week of August 20XX
Field Audit Testing	By 3rd week of August 20XX
Issuance of Draft Report	By 1st week of September 20XX
Issuance of Final Report	By 2nd week of September 20XX (Subject to receipt of management responses)

Do let us know your inputs, if any, on the above.

Our Staff Mr. XXXXXX will coordinate with you in this audit assignment.

Regards,

XXXXXXXXX

Audit Senior Manager, M/s ABC & Co Chartered Accountants.

Though the communication is agreed upon as above, in the actual conduct of audit there could be a situation which warrants immediate communication with the management considering the sensitivity of the matter. It could be verbal or written depending on the circumstance.

It is advisable to decide the format, template and medium of communication upfront to ease its execution.

Communication with Management and Those Charged with Governance (TCWG) (Refer SIA 290)

The internal audit function ultimately reports and is accountable to the Audit Committee. It is a desired and well established practice to proactively share the pertinent issues with the TCWG for their action before the actual meeting

date. This enables them to go through the issues well in advance. It is important to note that the levels of communication/ reporting before the TCWG communication, would vary from entity to entity. This is largely dependent on the size, complexity and legal structure of the entity.

This aspect is covered in SIA 290, which elaborates mainly on the following aspects:

(a) TCWG may include various levels of management with whom communication needs to be done. This also depends on the approved audit plan and charter. However, a process for communication with TCWG should be defined to ensure sustainability.

(b) The scope, objectives, frequency and other protocols for communication should be agreed with TCWG. In case of very urgent matters an emergency/ urgent communication protocol should also be agreed.

(c) The process and protocol may include aspects relating to Mode (verbal, written, Electronic), Channel (VC, email, phone, written), Timelines (emergency, weekly, etc.), Content (status, findings, hurdles), Participants (operational, HODs).

(d) The objective of communication is to mainly inform, persuade and act on important matters.

Who should communicate?

Auditing large and complex organizations require single point of contact, coordinators, preparing contact list of people who will participate in the internal audit, etc. This helps in achieving streamlined execution of an audit as well as ensuring that certain communications are initiated by the designated people only.

(Refer Standard on Internal Audit (SIA) 290, Communication with Management and Those charged with governance (TCWG))

Presentation and Communication of Internal Audit Report (Refer SIA 310)

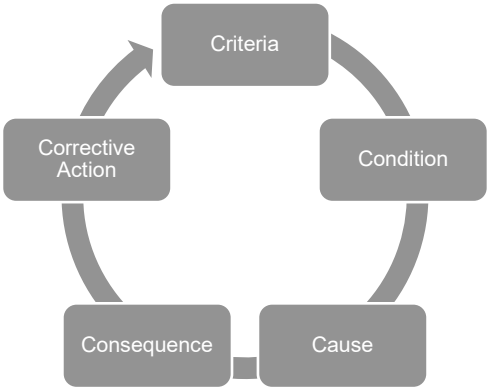
5.7 Internal Audit report shall contain:

- **Scope:** Areas covered, specific risk dimensions, period, etc.

- **Audit Approach:** Methodology used (e.g. sample testing, analytical, etc), fact that audit is performed per SIAs,
- **Executive Summary:** It is a high level summary of audit observations, enlisting material issues noted, which may have adverse effects (financial or non-financial) on the business.
- **Detailed Observations:** This section shall give more descriptive information about the observation, along with sample or examples noted as deviations, the root cause of the issue (reason of why such deviation took place), risk/implication it has on the overall business and recommendation to rectify the lapse in the process/control.
- **Conclusion:** This is overall opinion of an auditor, considering the observations, population it can impact, severity of the issue and risk levels involved with such observations.

Finalising Observations

On evaluation of evidence, the internal auditor then can finalise the observations noted during testing. The 5Cs of internal audit are key principles that guide the conduct and quality of internal audit reporting. These principles help ensure that audits are thorough, effective and valuable to the organization.



1. **Criteria:** The standards or benchmarks against which the audit is conducted. This includes policies, procedures and regulations that the organization must comply with.
2. **Condition:** The current state of the processes or controls being audited. This involves identifying any deviations from the criteria.

3. **Cause:** The root cause of any identified issues or deviations. Understanding why a problem occurred is crucial for addressing it effectively.
4. **Consequence:** The impact of the identified issues on the organization. This helps in understanding the severity and potential risks associated with the issues.
5. **Corrective Action:** Recommendations for addressing the identified issues and preventing their recurrence. This is essential for continuous improvement.

These principles help internal auditors provide clear, concise and actionable insights that can drive positive changes within the organization.

Observations noted are then to be discussed with the field management to validate the facts.

Specimen Internal Audit Observation

<table>
<tr><td>Observation title: Bank reconciliation statement not prepared for 3 months in respect of XXXX Bank. Average bank balance is ₹ XXXXXXXX.</td><td>Observation classification
<table><tr><td>Strategic</td><td>Financial</td><td>Operating</td><td>Compliance</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>Observation rating
<table><tr><td>High</td><td>Medium</td><td>Low</td></tr></table></td></tr>
<tr><td>Review of bank account reconciliations for XXX bank accounts revealed that the bank reconciliation statement was not prepared for Bank account # XXXXXX for Oct, Nov and December XXXX. This bank account is mainly used for making supplier payments for Plant XXXXX. Average balance during FY XX-XXXX was ₹ XXXXXXXXX (This is a Condition i.e. what is a fact or what has</td><td>Management Response:</td></tr>
</table>

actually happened)	
As per the Company's policy, the bank reconciliation is to be performed on a monthly basis. ***(This is a Criteria i.e. what should happen)***	Responsibility:
It was informed to us that this was due to non-availability of a designated person due to medical emergency at his end. ***(This is a cause)***	Target Date for Implementation:
Since this account is used for supplier payments, non-reconciling the bank balance with the book balance on a monthly basis, exposes the Company to the non-detection of incorrect payments, duplicate payments etc. ***(This is a consequence)***	
The company should consider the significance of the monthly control of bank reconciliation and accordingly, ensure alternate mechanism to perform bank reconciliation on a monthly basis. In respect of Oct, Nov and Dec XXXX, undertake detailed scrutiny of transactions to establish that these transactions have been performed/	

recorded accurately and completely in line with the Company's intent and authorizations' structure. ***(This is a Corrective action or a recommendation)***	

(Refer Standard on Internal Audit (SIA) 310, Presentation and Communication of Internal Audit Report.)

It is important to note that in a risk based internal audit,

- Audit assignment level risks are classified as per their significance
- More audit emphasis is put on the areas that have high risks
- Accordingly, the level of audit procedures i.e. nature, timing and extent, are determined
- Audit conclusions are evaluated to see if the underlying risks are mitigated or there are risk exposures that may create challenge in achieving one or more business objectives i.e. producing reliable financial information, using entity's resources economically, comply with the regulatory requirements and ensuring safeguarding of assets.

Since risk based internal audit requires more emphasis as per the significance of the risk, it implies that there could be many layers of audit procedures which will have to be performed having noted an audit exception.

Example:

XYZ Company pays commission to their distributors as per the volume of sales they undertake. The percentages of commission are fixed from time to time by the senior management of the Company.

Audit of distributors' transactions revealed payment of higher percent of commission than prescribed. Further verification revealed that such higher percent of commission was noted only for select locations and for select products only.

It was then understood that the products for which the higher percent of commission was paid were newly introduced in the selected areas considering local demand/ customer preferences. Since these products were new, distributors were little skeptical about building their inventory.

Therefore, the Company offered higher percent of commission for these products. This was duly authorized by the Company's Chief Executive Officer.

To reconfirm the above, internal audit team collected corroborative evidence of increase in the advertisement spend during last six month on these new products, especially in the areas where the higher percent of commission was paid.

Quality Standard on Internal Audit (Refer QSIA 1 and SIA 290)

5.8 Even though the management is responsible for acting on the audit observations and recommendations, the Internal Auditors are usually responsible for monitoring and reporting of prior audit issues. These monitoring and reporting activities are important since if these action plans are not implemented, the organization's risk exposure is not sufficiently mitigated and the value of the internal audit function is less likely to be realized.

It mainly covers following aspects:

- The method and timing of follow-up and roles and responsibilities should be formally agreed upon with the organization.
- The actions taken are as agreed and address the mitigation of the risk. Different actions, if taken, need to be appraised to TCWG.
- Use of IT systems/ technology can also be done for reminders and follow up and maintaining status etc.
- These activities can be done along with regular Internal Audit assignments or as a separate activity.
- Differentiated protocols can be used for closure of critical issues, medium risk and low risk issues.
- Reporting the status to TCWG and escalate in case of delays also with reasoning.

The Chief Internal Auditor, being responsible for continuous monitoring over closure of audit issues, needs to plan formal process to conclude the prior issues. In case of sensitive or critical issues, follow up audit shall be

performed (i.e. reperforming audit procedures on the samples/population from post-implementation period).

Escalation: In spite of regular follow up with the auditee or user department, if the corrective measures are not planned or implemented, then the auditor shall escalate the matter with the senior management or TCWG, highlighting the aging of the pending issues and impact it might have created in absence of corrective actions.

Timely and appropriate documentation at every stage, will help auditor to keep track of the date on which issue was first raised, stakeholders marked in the communication, follow up actions taken, frequency of follow up and escalations. This will help in creating an impact on severeness of the issue and safeguard auditor's position and fulfilment of responsibilities.

(Refer Standard on Internal Audit (QSIA) 1, Quality Standard on Internal Audit)

Content of Audit Report

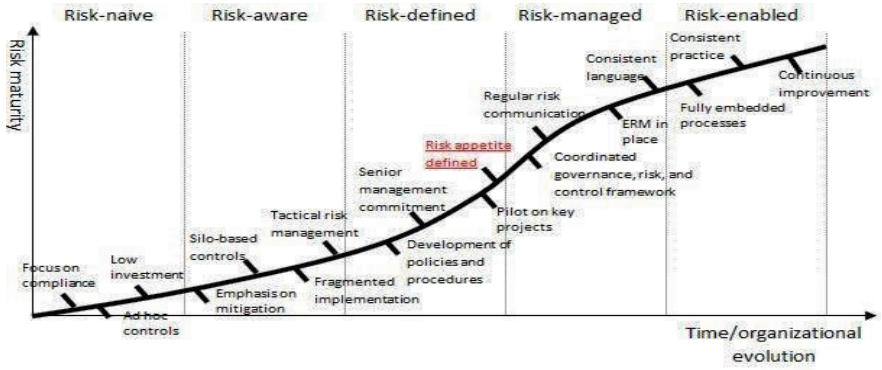
The audit report should include the following :

- Covering letter
- Scope
- Objectives
- Audit approach and methodology
- Overview of the audit area and legends for acronyms used in the report
- Details of the internal audit team and auditees
- Omissions, disclaimers, escalations
- Executive summary
- Detailed observations and annexures

Annexures

Annexure 1: Risk Maturity Table

	Risk maturity	**Risk-aware**	**Risk defined**	**Risk managed**	**Risk enabled**
Key characteristics	No formal approach developed for risk management	Scattered silo-based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined	Enterprise approach to risk management developed and communicated	Risk management and internal controls fully embedded into the operations
Internal Audit approach	Promote risk management and rely on alternative audit planning method	Promote enterprise-wide approach to risk management and rely on alternative audit planning method	Facilitate risk management/ liaise with risk management and use management assessment of risk where appropriate	Audit risk management processes and use management assessment of risk as appropriate	Audit risk management processes and use management assessment of risk as appropriate


Risk-naive
Risk-aware
Risk-defined
Risk-managed
Risk-enabled
Risk maturity
Time/organizational evolution
Focus on compliance
Low investment
Ad-hoc controls
Silo-based controls
Emphasis on mitigation
Tactical risk management
Fragmented implementation
Senior management commitment
Development of policies and procedures
Risk appetite defined
Pilot on key projects
Regular risk communication
Coordinated governance, risk, and control framework
Consistent language
ERM in place
Consistent practice
Fully embedded processes
Continuous improvement

Annexure 2: Risk Heat Map Matrix

Whatever approach is followed, the Risk Management exercise comes up with the Risk Heatmap during the risk evaluation process, where each risk is assessed with its likelihood and impact it would have on the organisation against the defined criteria/ risk appetite. Following is an example of such risk matrix where downside risks (adverse) and upside risks (opportunities) are plotted which can be used to develop the risk heatmap.

Example of Risk Matrix

Consequence	**Severe**	High	High	Extreme	Extreme	Extreme
	Major	Moderate	Moderate	High	High	Extreme
	Moderate	Moderate	Moderate	Moderate	High	High
	Minor	Low	Low	Moderate	Moderate	Moderate
	Insignificant	Low	Low	Low	Low	Moderate
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
	Likelihood					

Example of Organizations' Risk Heat Map

Risk Scoring	**Impact**	**Insignificant**	**Minor**	**Medium**	**High**	**Catastrophic**
Probability (%)	Rating scale	1 <.05	2 0.06 to 0.10	3 0.11 to 0.30	4 0.31 to 0.70	5 > 0.71
Very Likely	5	5	10	15	20	25
Likely	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Unlikely	2	2	4	6	8	10
Rare	1	1	2	3	4	5

Annexure 3: Audit Universe Format

Sr No	Business Cycle	Audit Area	Likage to Organisational objectives	Inherent Risk	Residual Risk	Value at Risk	Last Audited In Year	Last Audit Rating	Covered in Other LODs / Audits	Key Risk Factors	Priority	Other Remarks

Annexure 4: Audit Committee Requirement in India

Section 177 of the Companies Act, 2013 states the Board of Directors of every listed public company and such other class or classes of companies, as may be prescribed, shall constitute an Audit Committee

The Audit Committee shall consist of a minimum of three directors with independent directors forming a majority. Provided that majority of members of Audit Committee including its Chairperson shall be persons with ability to read and understand, the financial statement.

In India, Audit committee constitution is mandatory for all public companies having:

- a paid-up capital of Rs 10 crore or more or
- a turnover of Rs 100 crore or more
- outstanding loans or borrowings in excess of Rs 50 crore.

Sample Risk Based Internal Audit Framework

1. RISK BASED INTERNAL AUDIT (RBIA) METHODOLOGY AND FRAMEWORK

The risk-based annual Audit Plan shall also channel audit resources by prioritization of audits. This is conducted by the following steps:

Step 1: Identification of Audit Universe

Step 2: Conducting Risk Assessments

Step 3: Determining the Frequency of Audit

Stepwise Methodology for Risk Based Internal Audit Plan

Step 1: Identification of Audit Universe

An audit universe is the collective grouping of auditable 'components' also called auditable areas, units or entities that support the development of the Risk based Internal audit plan and helps to identify appropriate internal audit coverage which can then be prioritized.

The audit universe covers all auditable units within the Company. It includes all products and associated processes by the Company as well as all supporting functions complementing them. The audit universe will change according to changes in product offering, new controls/processes implemented as well as new functions created. The internal auditor should periodically review the audit universe to identify any changes therein and make necessary amendments, to make the audit plan responsive to those changes.

(i) Risk assessment will be conducted for all the individual audit units/ functions identified as part of Audit Universe.

(ii) The risk assessment of business and other functions of the organization shall at the minimum be conducted on an annual basis.

Step 2: Identification of Inherent Risks and Exiting Controls:

To ensure holistic coverage of all the activities under the functional/ unit/ departmental an independent risk assessment needs to be performed and for this the initial step to be undertaken is to document all the risks and

associated controls in the form of Risk Control Matrix (RCM) for such function/ unit/ department. Thus, to prepare such RCM following steps will have to be performed:

(i) Understanding of documented policy and procedure of the respective unit under assessment.

(ii) Understanding and reviewing of the existing RCM designed and maintained by the management.

(iii) Conducting walkthrough with key process owners, wherever required, to identify any gaps wherein, additional documentation is required in the existing RCMs.

(iv) Discuss and suggest suitable additional documentation for mitigating the gaps identified.

(v) Collaborate with the key process owners along with reference to the documented policy/ procedure, document the suggested risks and controls for mitigating the gaps identified.

Inherent Risk – Impact and Likelihood Assessment

Inherent business risks indicate the intrinsic risk in a particular area/activity of the organization and will be grouped into low, medium and high categories depending on the severity of the risk. Inherent risk rating will be done based on the impact and likelihood of a particular risk rating.

Inherent Risk Rating = Frequency of Control * Impact/ Severity of Risk

Inherent Risk Scores at each Risk Level

Frequency of Control			Scoring for Impact/ Severity of Risk	
Activity of Risk	**Score**		**Impact/ Severity**	**Risk Rating**
Annual	1		Incidental	1
Half Yearly	2		Minor	2
Quarterly	3		Moderate	3
Monthly/ One time	4		Major	4
Daily/ Weekly/ Fortnightly/ Ongoing/ Event Based	5		Extreme	5

Note:

Impact assessment will be undertaken using a combination of impact considerations given that certain risks may impact the enterprise financially while other risks may have a greater impact to reputation or safety. Each inherent risks will be rated on an impact scale 1-5. When assigning an impact rating to a risk, consideration will be given to assign the rating for the highest consequence anticipated. For example, if any one of the criteria for a rating of 5 is met, then the impact rating assigned is 5 even though other criteria may fall lower in the scale.

Inherent Risk Grading at each Risk level

Inherent Risk Rating Grid		
Lower Band	**Upper Band**	**Category**
0	5	Low
6	12	Medium
13	25	High

Inherent Risk Grading at each Auditable Unit

Inherent Risk Rating Average Score = Total Inherent Risk Score/ Total Count of Risk

Inherent Risk Grading Grid		
IR Average Grid		
Lower Band	**Upper Band**	**Category**
0	10	Low
11	15	Medium
16	25	High

Control Assessment – Design & Operating Effectiveness Strength

Control risks arise out of inadequate control systems, deficiencies/ gaps and/ or likely failures in the existing control processes.

Control Risk Scores at each Risk Level

Control Risk Rating = Design Effectiveness * Implementation Effectiveness * Operating Effectiveness

Design and implementation effectiveness of a control is concerned with evaluating whether that control is suitably designed to prevent, or detect and correct, material misstatements.

Operating Effectiveness of internal controls is concerned with assessing how the control was applied, the consistency with which it was applied during the audit period and who applied the control.

Control Risk Rating Grid		
CR Average Score		
Lower Band	**Upper Band**	**Category**
0	6	High
7	12	Medium
13	25	Low

Final Control Risk Grading at each Auditable Unit

Control Risk Rating Average Score = Total Control Risk Score/ Total Count of Risk

Control Risk Rating Grid		
CR Average Score		
Lower Band	**Upper Band**	**Category**
0	6	High
7	12	Medium
13	25	Low

Control Strength Scoring Matrix

		Design Effectiveness				
Operating Effectiveness		**Excellent**	**Good**	**Fair**	**Limited**	**Weak**
		5	**4**	**3**	**2**	**1**
Excellent	**5**	25	20	15	10	5
Good	**4**	20	16	12	8	4
Fair	**3**	15	12	9	6	3

Limited	**2**	10	8	6	4	2
Weak	**1**	5	4	3	2	1

Residual Risk Assessment

The residual risk is the level of risk associated with an activity after proposed/ additional controls have been implemented to further eliminate or reduce the inherent risk.

Residual Risk = Inherent Risk Score – Control Score

Qualitative Assessment

The risk assessment may make use of both qualitative and quantitative approaches. While the quantum of credit, market and operational risks will be largely determined by quantitative assessment, the qualitative approach will be adopted for assessing the quality of overall governance and controls in various business activities.

The risk assessment methodology includes, inter alia, the following parameters:

(a) Previous internal audit reports and open issues

(b) Proposed changes in business lines or change in focus

(c) Significant change in management/ key personnel

(d) Results of latest regulatory examination report

(e) Reports of external auditors

(f) Industry trends and other environmental factors

(g) Time lapsed since last audit

(h) Volume of business and complexity of activities

(i) Substantial performance variations from the budget

Following steps are preformed to arrive at final Inherent Risk Rating as per Qualitative Assessment Model:

- Scores and Indicative Parameters are assigned to the Qualitative Assessment Categories (tabulated below).
- Scores are then assigned to each qualitative assessment category basis the auditable units to arrive at the qualitative assessment inherent risk rating (inherent risk of other factors).

- The inherent risk of other factors is combined with the Inherent risk rating for each auditable units determined at point 2.1 to obtain Inherent Grading (Matrix given below).
- Inherent Grading of unit and Control Risk is then combined to determine the frequency of each auditable units.

Qualitative Assessment Categories with Scores and Indicative Parameters

Qualitative Category	Score	Indicative Parameter
Open High Risk Internal Audit/ IFC observations > 90 days in the previous year	1	No High/ Medium level issue reported in last audited report
	2	At least 1 High/ Medium level issue reported in last audited report
	3	More than 2 High/ Medium level issues reported in last audited report
Proposed changes in business lines or change in focus	1	No notable change under contemplation
	2	Not applicable
	3	Anticipated changes in business lines/ functions/ technology
Significant change in management/ key personnel	1	No change in Sr. Management/ Key Personnel in past 1 year
	2	Not Applicable
	3	Change in Sr. Management/ Key Personnel in past 1 year
Results of latest regulatory examination report	1	No regulatory observation noted in the area from the last audited report
	2	Regulatory observation noted in the area from last audited report
	3	Repeated regulatory observation noted in the audit report

Qualitative Category	Score	Indicative Parameter
Reports of external auditors	1	No observation noted in the area from last audited report
	2	Observation noted in the area from last audited report
	3	Repeated observation noted in the audit report
Risk arising due to Industry trends and other environmental factors impacting unit	1	Key activities do not get impacted by any change in Industry trends and other environmental factors
	2	Key activities get limited impact of any change in Industry trends and other environmental factors
	3	Key activities subject to substantial impact of any change in Industry trends and other environmental factors
Time elapsed since last audit	1	Audited in last 1 year
	2	Audited in last 2 years
	3	Audited more than 2 years ago
Volume of business and complexity of activities	1	Key activities do not directly impact volume of business transactions (E.g. - Oversight Functions)
	2	Key activities with limited usage of tools/ techniques/ process directly impacting volume of business transactions (E.g. - Business Function - Sales, HR)
	3	Key activities with usage of tools/ techniques/ process directly impacting volume of business transactions (E.g. - IT, Operations, Credit, etc.)

Qualitative Category	Score	Indicative Parameter
Performance variations from the budget	1	No notable variation
	2	Moderate variation
	3	Major Variation

Final Inherent Grading

Inherent Risk – Risk Matrix	Inherent Risk of Other factors	Concat	Inherent Risk Grading
Low	Low	LowLow	Low
Low	Medium	LowMedium	Medium
Low	High	LowHigh	High
Medium	Low	MediumLow	Medium
Medium	Medium	MediumMedium	Medium
Medium	High	MediumHigh	High
High	Low	HighLow	High
High	Medium	HighMedium	High
High	High	HighHigh	High

Risk Grading of Auditable Units

Risk Rating of Auditable unit = Outcome of Final Inherent Grading* Outcome of Control risk

Each auditable unit would be plotted on a heat map, basis on which the frequency of each audit will be determined.

Inherent Business				
	HIGH	A Medium	B High	C High
	MEDIUM	D Medium	E Medium	F High
	LOW	G Low	H Medium	I Medium
	Parameters	LOW	MEDIUM	HIGH

Control Assessment

Frequency of Audits

The frequency of the audits shall range up to three years from the last financial year and may vary for different functions depending on the composition, nature, size and regulatory requirements.

Frequency of risk assessment matrix is as below:

Final Risk Rating	Frequency of Audit
High Risk	Once in 6 Months
Medium Risk	Once in a Year
Low Risk	Once in 18 Months

While finalizing the frequency of audit units, the IAD shall also consider the previous report rating of the audit unit. The IAD shall select the frequency (basis the risk rating) which is more conservative.

The annual audit plan shall be revisited to incorporate likely changes in the business environment and adjustments shall have to be made based on new or changed risk factors.

2. QUALITY ASSURANCE IN INTERNAL AUDIT

Responsibilities of CIA to perform Quality Assurance

The Audit Committee/ Board should formulate and maintain a quality assurance and improvement program that covers all aspects of the Internal Audit function. The Internal Audit function must ensure adherence to the Quality Assurance and Improvement Program and undertake assessment of the Internal Audit function at least once in a year for adherence to the internal audit policy, objectives and expected outcomes.

Quality Assurance Framework

(i) An independent person/ firm conducts quality assurance of the audits performed

(ii) Review the RBIA to ensure that the Internal Audit Plan is comprehensive

(iii) Review of working papers to ensure the following:

- (a) Audit Programme
- (b) Sampling Rationale
- (c) Checklists
- (d) Reporting of Observations
- (e) Status of Open Issues

ISBN: 978-93-47892-02-8

www.icai.org