

# Overall Internal Audit Planning

(SIA 220 - Conducting overall internal audit planning  
and  
IIA Standard 2010 – Planning, 2020- Communication and Approval,  
2030 - Resource Management & 2040 - Policies and Procedures)

CA Kalpesh Panchal

Intensive Refresher Course on Internal Audit (Virtual) organised by WIRC of ICAI  
Presentation on 15<sup>th</sup> July 2022

# Table of Contents

Backdrop

Challenges faced by internal auditor

What is Risk ?

What is Audit Universe?

What is Risk Based Internal Audit [RBIA]?

Process of RBIA Planning

Test Your Knowledge

Resources used



Backdrop

# Backdrop

- Need of strong and robust internal auditing and internal control systems due to increase in the trend of frauds in the corporate sector.
- Regulators have also become more vigilant towards the requirement of strong internal control system and the need for risk based internal audit. *[viz., Sarbanes Oxley Act in USA, Clause 49 of Listing Agreement as per SEBI, Companies Act, 2013]*
- Risk-based Internal Auditing (RBIA) allows internal auditor to provide assurance to the Board of Directors that risk management processes are managing risks effectively.

# Changes in Definition of Internal Audit

1947	1981	1999
<p>Independent <b>appraisal activity</b> within an organization for the review of accounting, financial and other operations as a basis for protective and constructive <b>service to management</b>.</p>	<p>An independent <b>appraisal function</b> established within an organization to examine and evaluate its activities as a <b>service to the organization</b>.</p>	<p>Internal auditing is an independent, objective <b>assurance and consulting activity</b> designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and <b>improve the effectiveness of risk management, control, and governance processes</b>.</p>

# Challenges faced by internal auditor

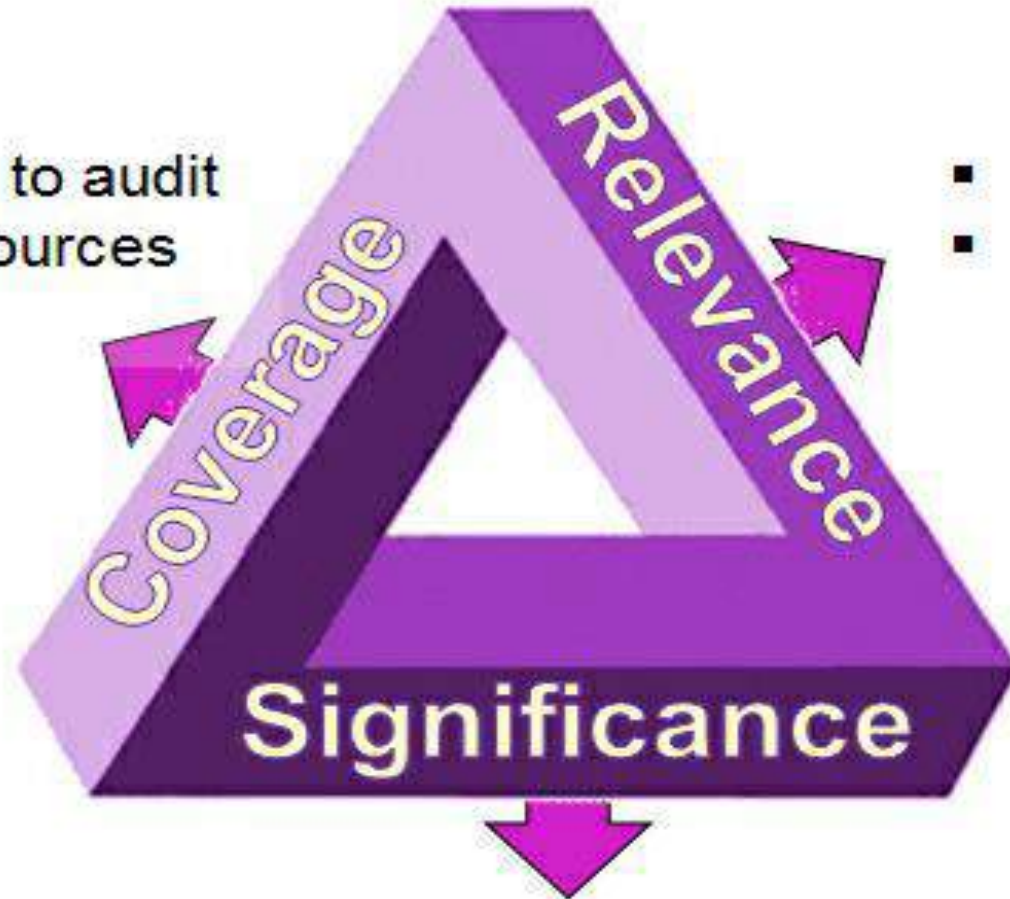
# Challenges Faced by Internal Auditor

- Mismatch in the expectations
- Audit risk
- Practical implementation of audit standards
- Size and complexity of data
- Uncertainties due to changing environment
  - Internal as well as external



# Three Axioms of Auditor's Dilemma

- How much to audit
- Use of resources



- What to audit
- Use of resources

- Depth of audit
- Use of resources



What is Risk?

# What is Risk?



- Risk is defined by IIA's International Standards of Professional Practices as:

*“The possibility of an event occurring that could have an impact on the achievement of objectives.”*

- Risk is defined by ISO 31000 as:

*“the effect of uncertainty on objectives.”*

**Source:**

International Standards on Internal Audit issued by the IIA – Page 24 (Glossary)  
<https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en> (Point 3.1 of “Terms and Definitions”)

# Relationship Between Inherent Risk & Residual Risk



## Risk management

- Accept
- Reduce
- Transfer
- Avoid

# What is Audit Universe?

# What is Audit Universe?

- As per SIA 220, prior to defining scope, a complete identification of **all auditable units** (locations, functions, business units, legal entities and relevant third parties) shall be made. This list is known as “**Audit Universe.**”
- Preparation of audit universe ensures that no auditable unit is overlooked.
- The audit universe and the related audit plan should also reflect changes in the management’s course of action, corporate objectives, etc.



# Information to be considered while preparing audit universe

Organization Strategy & Value Chain

All major areas, units, departments along with their objectives & strategies

Third Party Vendors

Major IT applications and Information System Assets

Regulatory and Legal Compliance Requirements

Non- financial performance indicators (Eg- environmental, health & safety)

**Source:**

# Steps for Preparation of Audit Universe



# Illustrative Audit Universe (Manufacturing Company)

Sr.No	Department	Locations					
		Head Office	Branch Office – 1	Branch Office – 2	Central Warehouse	Factory – 1	Factory – 2
1	Compliances	✓	✓	✓	✓	✓	✓
2	Maintenance					✓	✓
3	Human Resources	✓					
4	Production					✓	✓
5	Procure to Pay	✓			✓	✓	✓
6	Order to Cash	✓	✓	✓	✓		



What is RBIA ?

# What is RBIA ?

RBIA is an internal methodology which is primarily focused on the inherent risk involved in the activities or system and provides assurance that risk is being managed by the management within the defined risk appetite level.

## Traditional IA

Control assurance based  
on routine audit

## RBIA

Assurance on the  
effectiveness of risk  
management [in addition  
to control assurance]

# Advantages of RBIA

- Management has identified, assessed and responded to risks above and below the risk appetite
- The responses to risks are effective but not excessive in managing inherent risks within the risk appetite
- Where residual risks are not in line with the risk appetite, action is being taken to overcome the same
- Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively (\*)
- Risks, responses and actions are being properly classified and reported

**Source:**

(\*) Page 34 of the Guidance Note on RBIA issued by ICAI

# Process of RBIA planning

# Process of RBIA Planning



# Understand the Organization

Identifying objectives, strategies and structure

Reviewing key documents i.e. Organization chart, annual report, etc.

Consulting with key stakeholders i.e. Board of directors, management, HODs, etc.

# Identify, assess and prioritize risks



- Auditor shall carry out independent risk assessment of all auditable units in the audit universe.
- Based on this assessment, auditor can **prioritize & focus audit work on high risk areas** with due attention to matters of importance, complexity & sensitivity.

# Identify, assess & prioritize risks – Factors for Risk Assessment



**Source:**

Considerations for Implementation (IIA Standard 2010) – Page 96 and 97 of IIA's Implementation Guide



# Prioritize risks – Various types of risk

Non-compliance

Financial Loss

Health & Safety

Reputation

Fraud /  
misappropriation

Management's  
assertion

Impact on Profitability

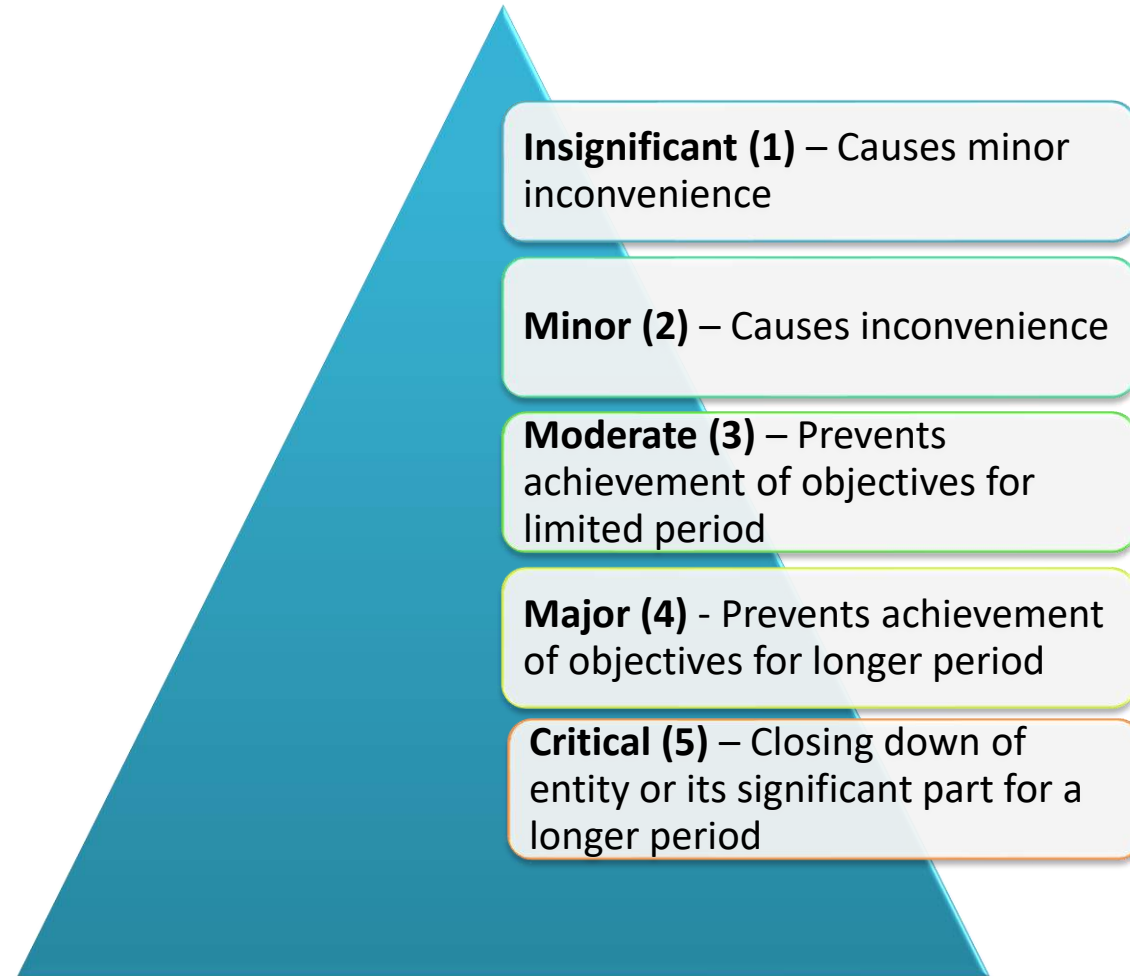
IT system

Complexity

Earlier audit  
observations

# Components of Risk Score – Impact of Risk

## Measurement Criteria for Impact of Risk

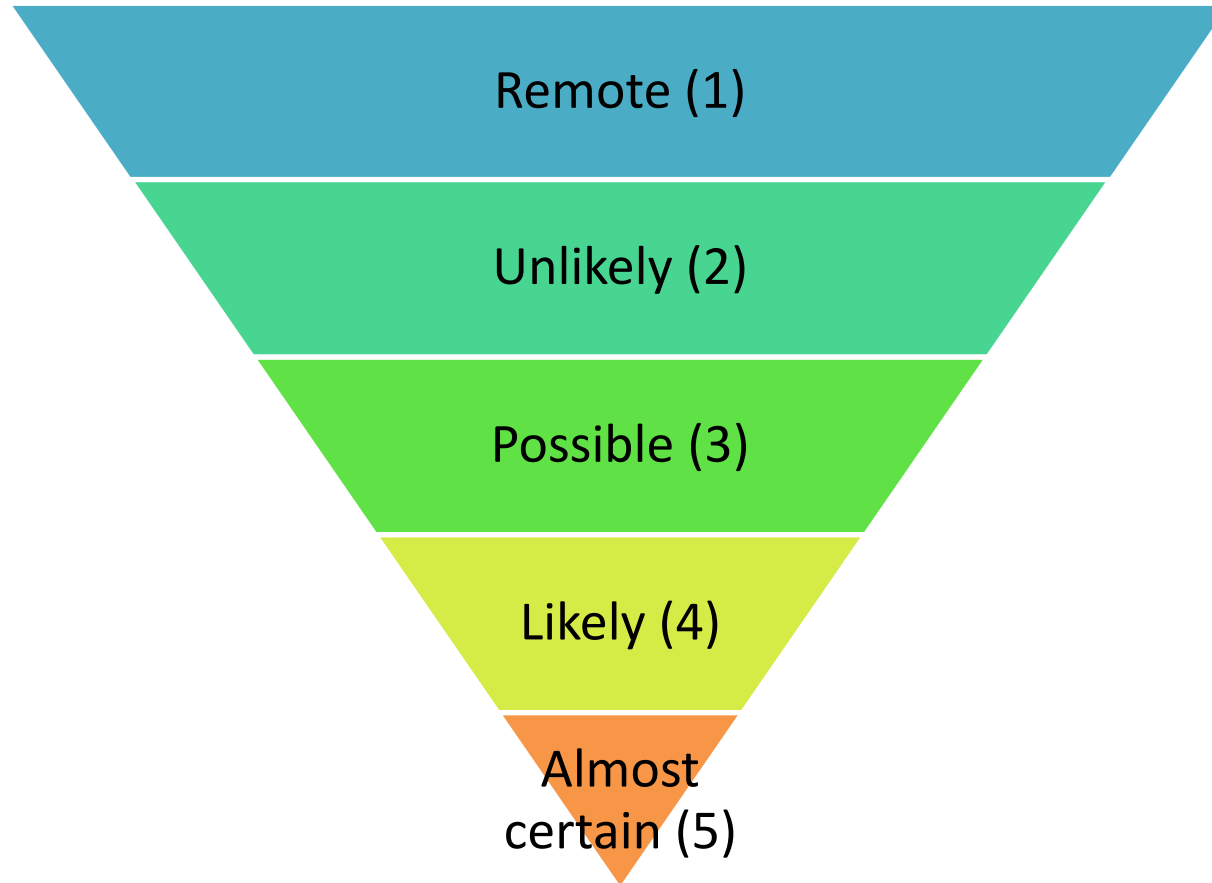


**Source:**

Exhibit 2 (Page 53) – Guide on Risk Based Internal Audit issued by ICAI

# Components of Risk Score – Likelihood of Risk

## Measurement Criteria for Likelihood of Risk



# Determining Risk Score for each area



<b>Likelihood of Risk</b>	Almost Certain (5)	5	10	15	20	25
	Likely (4)	4	8	12	16	20
	Possible (3)	3	6	9	12	15
	Unlikely (2)	2	4	6	8	10
	Remote (1)	1	2	3	4	5
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)

## Impact of Risk

# Allocate Resources

- As per SIA 220, Resource Allocation involves estimation of required time & skills for each area based on the attention it deserves (on the basis of risk assessment).
- The **requirement is matched with the competencies (i.e. knowledge, expertise and experience)** of resources available to identify any critical skill/expertise gaps in the audit team.
- As per IIA Standard 2030, these gaps can be filled by:
  - Training existing staff/requesting an expert guest auditor.
  - Co-sourcing/outsourcing engagements.
  - Hiring additional staff.



**Source:**

Para 4.7 of SIA 220 issued by the ICAI  
Considerations for Implementation (IIA Standard 2030) – Page 103 of IIA’s Implementation Guide

# Resource management – Factors to be considered

Number of internal audit staff and productive hours available

Consider knowledge, skill and other competencies of the internal audit staff

Fund available for training, technology, or additional staff

Availability of auditable entities

# Drafting internal audit plan – Points to be included

List of proposed audit engagements (specifying whether the same is assurance/consulting in nature)

Rationale for selecting each proposed engagement (E.g. - risk rating, time elapsed since last audit etc.)

Objectives & scope of each proposed engagement

Frequency/periodicity of each engagement

Risks to be addressed in each engagement

# Discussion with Process Owners – Points to be addressed

Have all risks & auditable units been considered exhaustively ?

Are there any upcoming changes which have not been considered ? (system upgrades, new software implementation etc.)

How do the engagements link to the objectives and top risks ?

How do the engagements add value to the organization ?

Any request of senior management which has not been considered ? (along with reasons thereto)



# Communicate final plan for approval

- As per IIA Standard 2020, the Chief Audit Executive (CAE) must communicate the internal audit plan and **resource requirements** (along with impact of resource limitations) including **significant interim changes** to senior management and board for review and approval.
- The CAE must clearly state the risks which cannot be addressed due to resource limitations.



# Assess risks continuously and update the plan

- Re-assessment of risks should be done at regular intervals to determine impact on audit plan.
- As per RBIA guide, areas where **new & significant risks** are identified may be **added** and areas where risks are **reduced** may be **removed**.
- As per SIA 220, significant changes to plan shall be done only after consultation with those who approved original plan.
- Such changes, reasons for changes & communications in relation to the same shall be documented.



**Source:**

Page 41 of Guide on Risk Based Internal Audit issued by the ICAI  
Para 3.6 of SIA 220 issued by the ICAI

# Illustrative RBIAP [For few department / activity]

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Control Environment Rating	Residual Risk Score	Frequency of Audit	Audit Plan Year - 1	Audit Plan Year - 2	Audit Plan Year - 3
				Corporate Office	Plant	Depot							
1	Contracts	1.1	Tendering and RFQ	✓			4.00	4.00	16.00	Every Year	✓	✓	✓
1	Contracts	1.2	Contracting and Ordering	✓	✓		3.80	4.00	16.00	Every Year	✓	✓	✓
2	Plant Operations	2.1	Production and Distribution		✓		3.91	3.00	12.00	Twice in 3 years	✓		✓
2	Plant Operations	2.2	Operation and Maintenance		✓		3.83	3.00	12.00	Twice in 3 years	✓		✓
2	Plant Operations	2.3	Safety and Environment		✓		4.50	3.00	14.00	Twice in 3 years	✓		✓
3	Drilling	3.1	Drilling		✓		3.80	4.00	16.00	Every Year	✓	✓	✓
4	Information Technology	4.1	IT Security	✓	✓		4.13	2.00	9.00	Twice in 3 years	✓	✓	✓
4	Information Technology	4.2	ERP and other applications	✓			3.43	2.00	7.00	Once in 3 years	✓		

# Practical tips on RBIA

Industry  
knowledge

80:20 principle

Judgement  
based on  
experience

Audit tools  
[Walk through,  
flow chart, etc.]

Focus on new  
development

Keep in touch  
with  
management

Refer RCM



Test Your  
Knowledge

# Test Your Knowledge

## 1. Overall internal audit plan shall be reviewed and approved by

- a) Chief Audit Executive and Audit Committee
- b) Chief Financial Officer and Board of Director
- c) Company Secretary and Audit Committee
- d) Board of Director or Audit Committee

### Answer – (d)

As per Para 3.2 of the SIA 220 issued by the ICAI, “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.”

# Test Your Knowledge

## 2. An Audit Universe shall be prepared:

- a) after establishing the scope of overall internal audit plan
- b) during the execution of the internal audit assignment
- c) prior to establishing the scope of the overall internal audit plan
- d) After the completion of the internal audit assignment

### Answer – (c)

As per Para 4.4 of the **SIA 220** issued by the ICAI, “Prior to defining the scope of internal audit, a complete identification of all the Auditable Units (locations, functions, business units, legal entities, including third parties where relevant) of the organisation shall be made.”

# Test Your Knowledge

**3. To develop the risk-based internal audit plan, the chief audit executive consults with senior management and the board and obtains an understanding of:**

- a) Organization's strategies
- b) Key business objectives
- c) Associated risks and risk management processes
- d) All of above

**Answer – (d)**

As international standard on internal audit **2010 – Planning** issued by IIA “To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes.”



# Test Your Knowledge

**4. The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to**

- a) Chief Financial Officer and Company Secretary
- b) Senior Management and the Board of Directors
- c) Chief Financial Officer and Chief Operating Officer
- d) Company Secretary and Statutory Auditor

**Answer – (b)**

As international standard on internal audit **2020 – Communication and Approval** issued by IIA, “The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.”

# Test Your Knowledge

**5. To achieve the objective of the approved internal audit plan, the chief audit executive must ensure that internal audit resources are:**

- a) Appropriate
- b) Sufficient
- c) Effectively deployed
- d) All of above

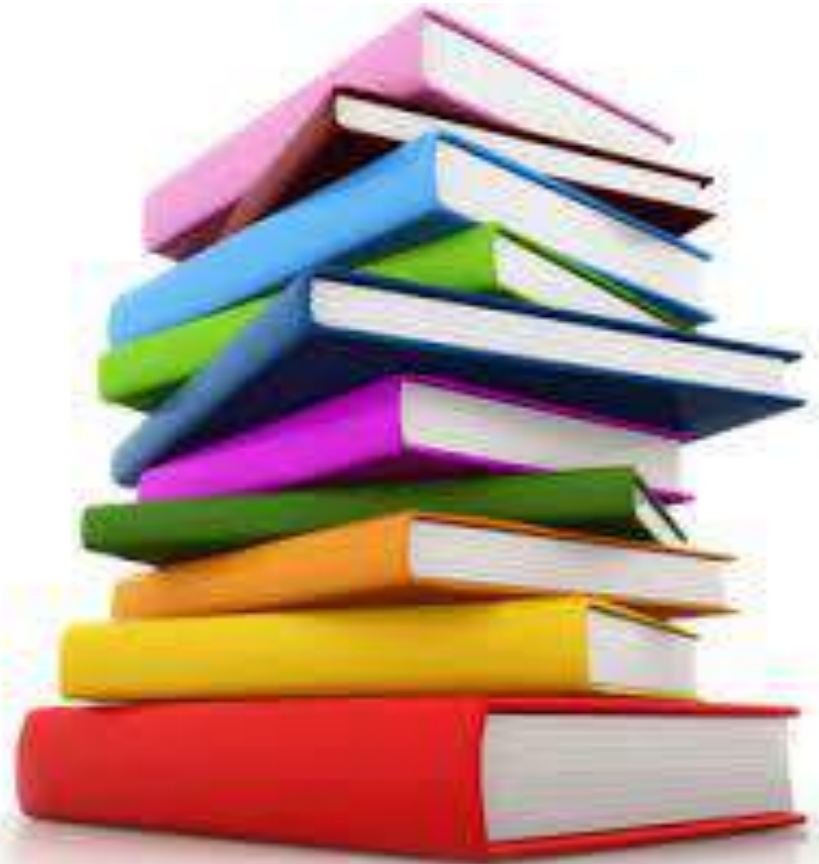
**Answer – (d)**

As per the international standard on internal audit **2030 –Resource Management** issued by IIA, “The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.”

# Resources

# Resources used for preparation of this presentation

- Standards on Internal Audit issued by ICAI
- International Standards on Internal Audit issued by the IIA
- Implementation Guide for the Standards issued by the IIA
- Guide on Risk Based Internal Audit issued by the ICAI
- Practice Guide on Developing Risk Based Internal Audit issued by the IIA
- Guidance Note on Risk Based Internal Audit issued by ICMAI
- [www.theiia.org](http://www.theiia.org)
- [https://en.wikipedia.org/wiki/Risk-based\\_internal\\_audit](https://en.wikipedia.org/wiki/Risk-based_internal_audit)
- <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>



Thank You

CA Kalpesh Panchal  
Kalpesh.Panchal@nashah.com