# Risk Based Internal Audit Plan

## (Developing a Risk based IA Plan and updating the Audit Universe)

C.A. Milan Mody

WIRC of ICAI
Presentation on 18th August 2018

"THE TRADITIONAL AUDITOR IS BARRELING TOWARD OBSOLETE, AND THEY GENERALLY DON'T EVEN REALIZE IT."

—FORRESTER

# Table of Contents

# Backdrop

# Backdrop

- Need of a 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 [viz., Sarbanes Oxley Act in USA, Clause 49 of Listing Agreement as per SEBI and Companies Act, 2013 and rules thereunder]

- 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 |
|---|---|---|
| Independent **appraisal activity** within an organization for the review of accounting, financial and other operations as a basis for protective and constructive **service to management**. | An independent **appraisal function** established within an organization to examine and evaluate its activities as a **service to the organization**. | Internal auditing is an independent, objective **assurance and consulting activity** 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 **improve the effectiveness of risk management, control, and governance processes.** |

Source : www.theiia.org

# What is Risk?

# What is Risk?

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

  *"The uncertainty 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"*

# Relationship Between Inherent Risk & Residual Risk


Inherent Risk

## Risk management

- Accept
- Reduce
- Transfer
- Avoid

# Key Focus Area Based on Emerging Risk

| | | | |
|---|---|---|---|
| Cyber security | Technology risk | Regulatory risk | Corruption |
| Corporate governance | Vendor governance | Crisis management planning | Culture / soft controls |

Source : IIA & Others

As per SIA -13 – The risk assessment process should be of a continuous nature so as to identify not only residual or existing risks, but also **emerging risks**.

# 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 RBIA ?

# What is RBIA ?

IIA defines risk based internal auditing (RBIA) as a methodology that links internal auditing to an organisation's overall risk management framework.

RBIA allows internal audit to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite.

# Traditional IA vs. RBIA

## Traditional IA

Control assurance based on routine audit

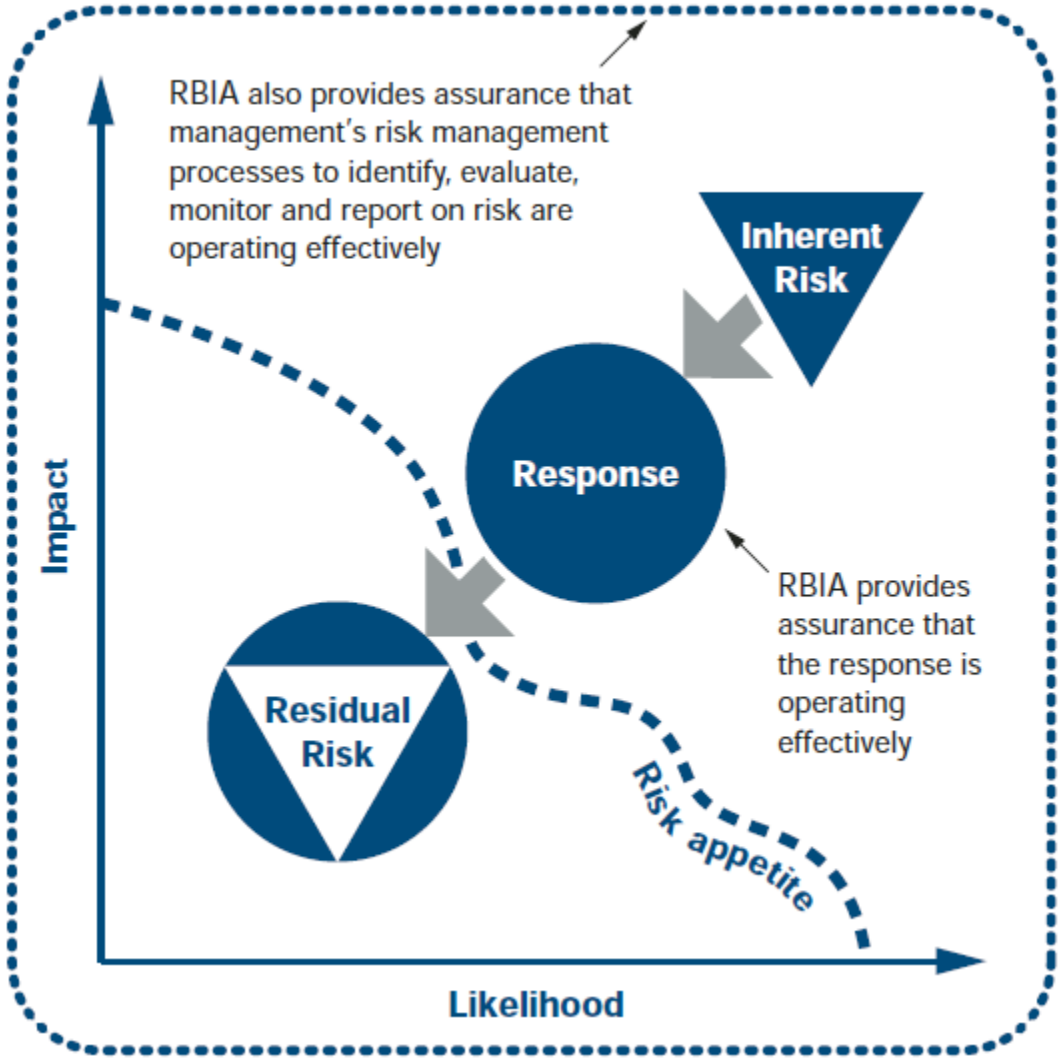
## RBIA

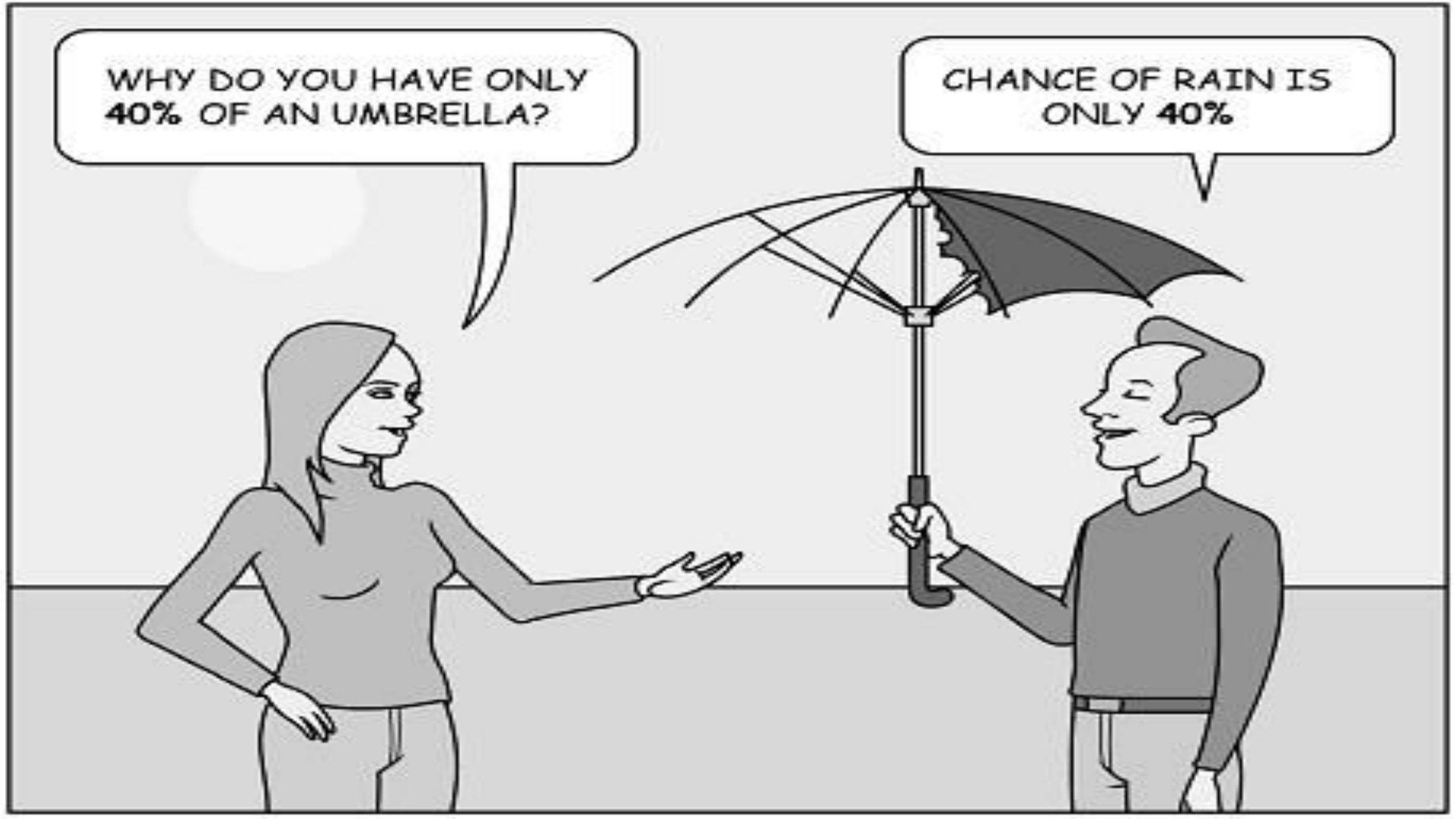
Assurance on the effectiveness of risk management [in addition to control assurance]

# Advantage 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 remedy that
- 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.

# Assurance Provided by RBIA



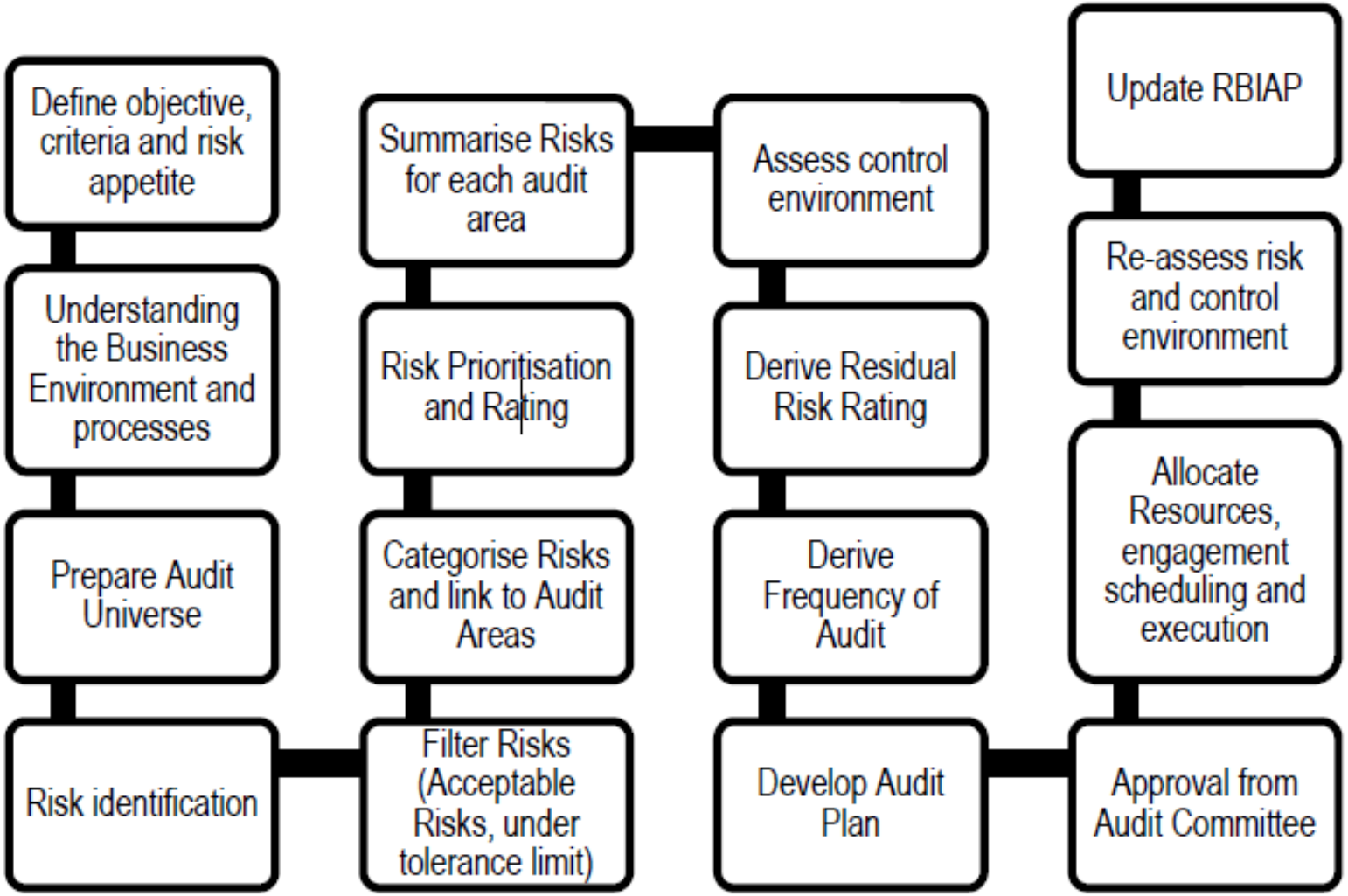

WHY DO YOU HAVE ONLY 40% OF AN UMBRELLA?
CHANCE OF RAIN IS ONLY 40%

# RBIA plan

# RBIA Plan [RBIAP]

- Responsibility of chief internal auditor of the Company
- Review on annual basis
- Approved by audit committee
- Needs to be consider:
  - Major risk
  - Business objective
  - Risk appetite
  - Inputs from key management
  - Business environment

# Process of RBIAP



# Define Objective, Criteria and Risk Appetite

| Objective | Criteria | Risk appetite |
| --- | --- | --- |
| • Size & nature<br>• Complexity<br>• Resource constraint | • Risk categorization<br>• Risk assessment<br>• Control environment<br>• Priority & frequency | • Discussion with management |

Risk rating depends on the criteria set by the organization to assess and prioritise its risk. Depending on the risk appetite of the organization, it could mean financial loss of 1 Lakh could be ‘minor’ for a large PSU with annual profit of 500 crores but it could be major for an organization with annual profit of 50 Lakh.

# Understanding the Business Environment and Processes

Understand business process

Feedback from management & audit committee

Comparison with market leader

Engage with all stack holders

# What is Audit Universe?

SIA 1 "Planning as Internal Audit" defines audit universe as "Audit universe comprises the ***activities*, operations, units**, etc., to be **subjected to audit** during the planning period. The audit universe is designed to reflect the overall business objectives and therefore includes components from the strategic plan of the entity. Thus, the audit universe is affected by the risk management process of the client. The audit universe and the related audit plan should also reflect changes in the management's course of action, corporate objectives, etc."

# Key Factors for Audit Universe

- Organisation objective
- Expectation from internal audit
- Organisation structure and set-up
- Geographic location of organisation
- Scalability of operation
- Organic linkage between business process
- Sufficiency to justify cost of control

# Steps for Preparation of Audit Universe

# Illustrative Audit Universe of a Manufacturing Company

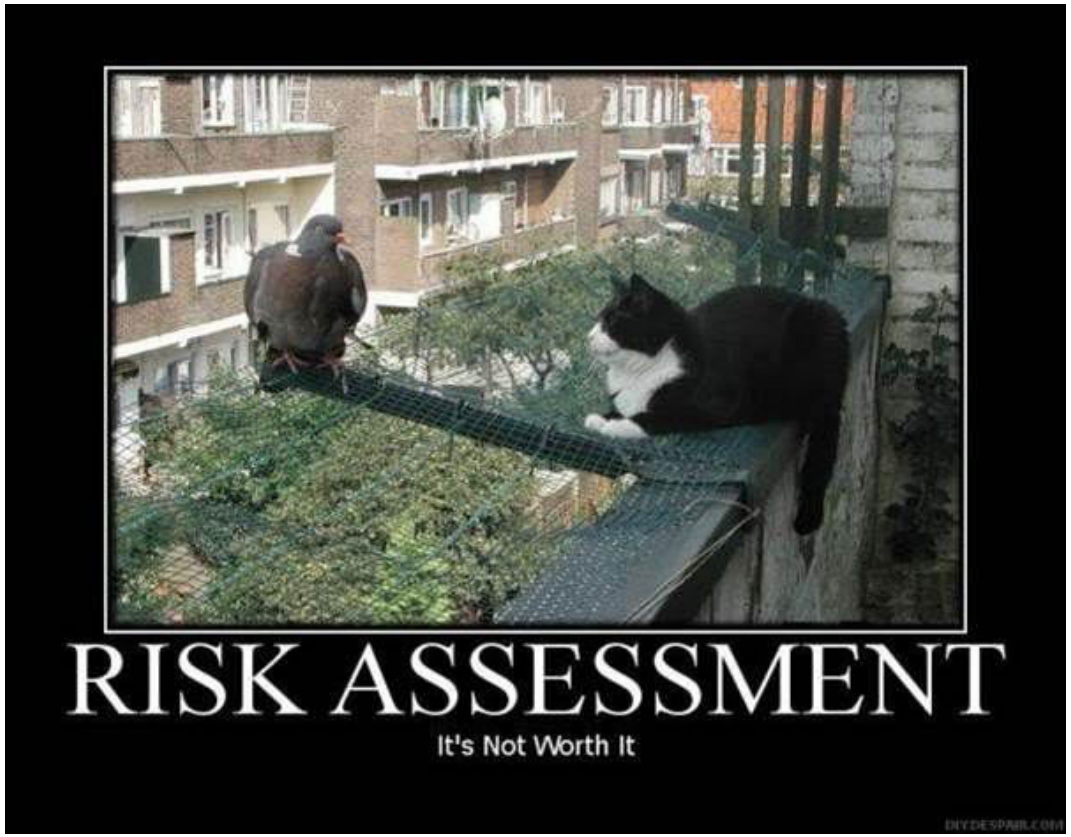
| *Sr. no.* | *Department* | *Business Locations* | | | |
|---|---|---|---|---|---|
| | | *Corporate Office* | *Plant* | *Branch Office 1* | *Branch Office 2* |
| 1 | Order to Cash | | | ✓ | ✓ |
| 2 | Procure to Pay | | ✓ | | |
| 3 | Human Resource and Payroll | ✓ | | | |
| 4 | Finance and Accounts | ✓ | ✓ | | |
| 5 | Production | | ✓ | | |
| 6 | Logistics and Distribution | | ✓ | ✓ | ✓ |
| 7 | Capital Expenditure | ✓ | | | |
| 8 | Plant Maintenance | | ✓ | | |
| 9 | Information Technology | ✓ | | | |
| 10 | Warehouse Management | | | ✓ | ✓ |
| 11 | Statutory Compliances | ✓ | ✓ | | |

# Risk Register

Risk register containing the list of all the risks identified and the preliminary risk rating.

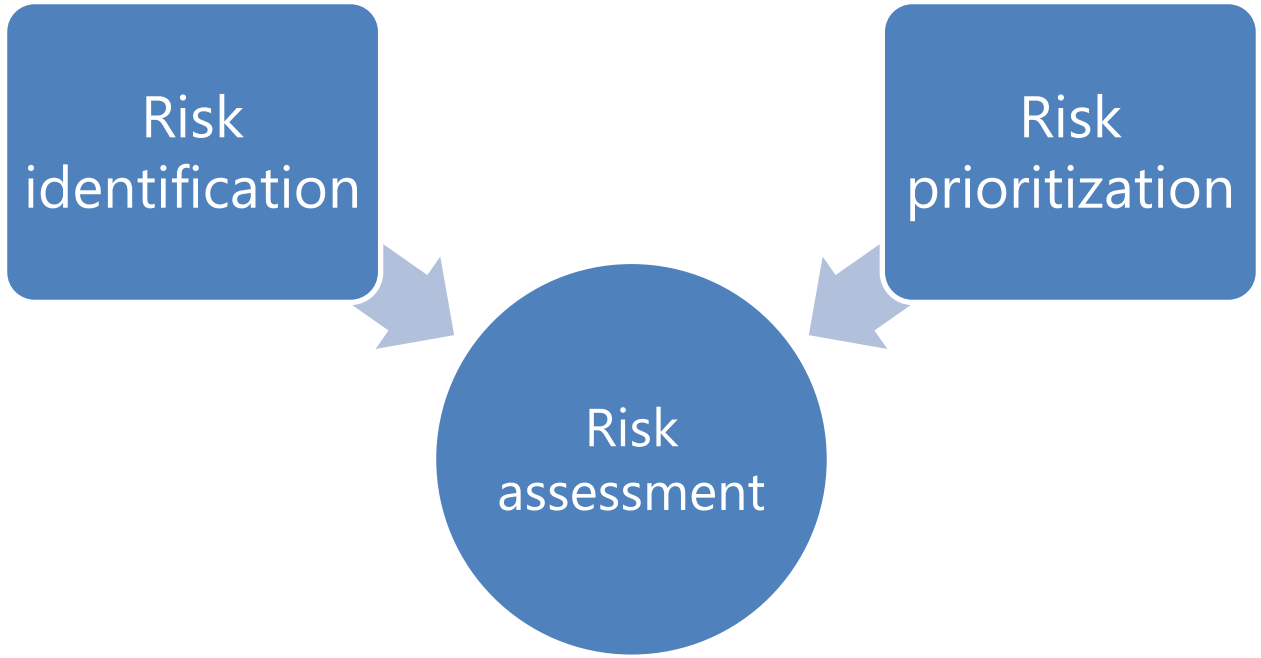
| Auditable Entity | Sub-Process | Risk Description | Risk Category | Risk Rating |
|---|---|---|---|---|

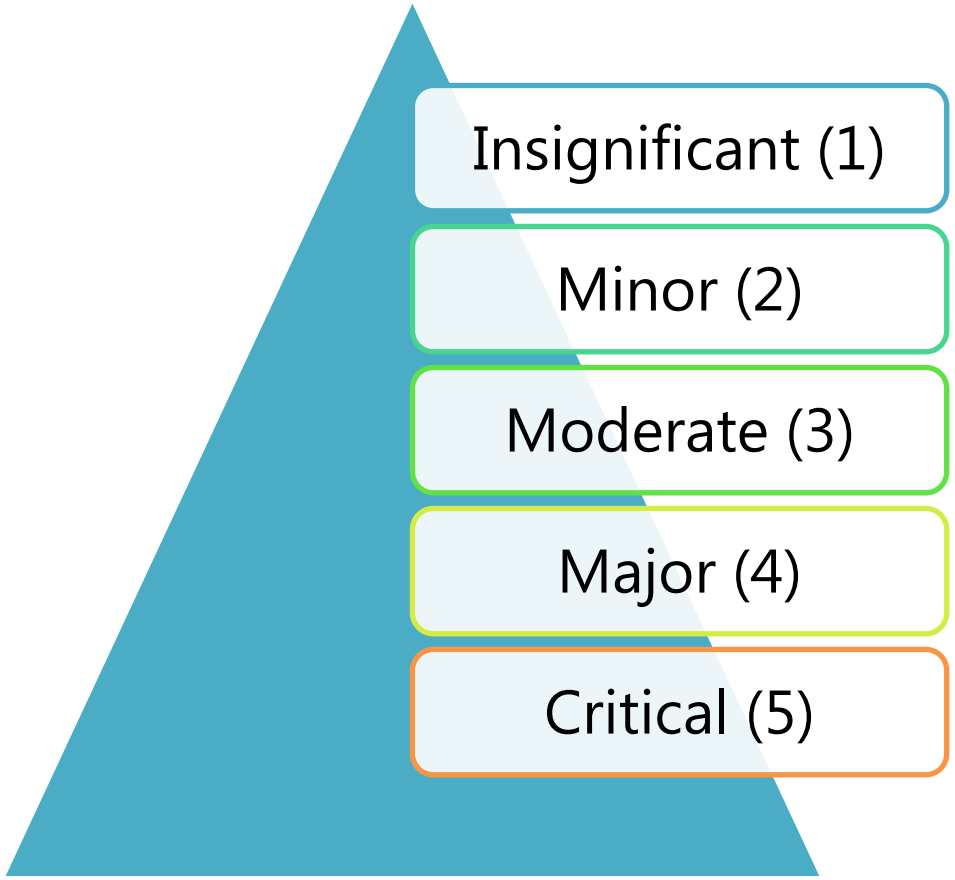
# Risk Assessment




- Non-compliance
- Financial Loss
- Health & Safety
- Reputation
- Fraud / misappropriation
- Management's assertion
- Impact on profitability
- IT system
- Complexity
- Earlier audit observations

# Risk Assessment (Continued…)



# What is control Environment

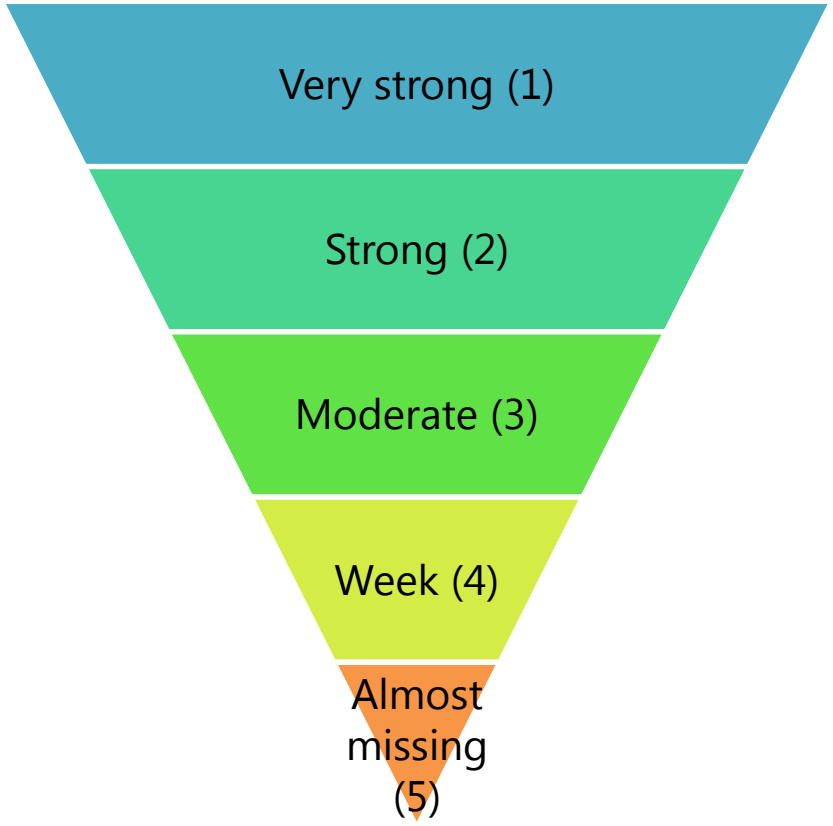
As per COSO, the control environment is the set of standards, processes and structures that provide the basis for carrying out internal control across the organisation.

As per SIA 12 "control environmen32t" means the overall attitude, awareness and actions of directors and management regarding the internal control system and its importance in the entity.

# Control Environment Rating

- Existence of preventive or detective control to mitigate risks associated with / mapped to the business process, entity or location.
- Legal compliance framework
- Appropriate and established IT Control environment
- Governance structure/ monitoring Mechanism
- Documented policy and procedures
- Past incidents/ trend
- Organization's sensitivity towards Health, Safety & Environment
- Fraud detection
- Balance of centralized versus decentralized operations within the organization

**Control Environment Rating Pyramid**



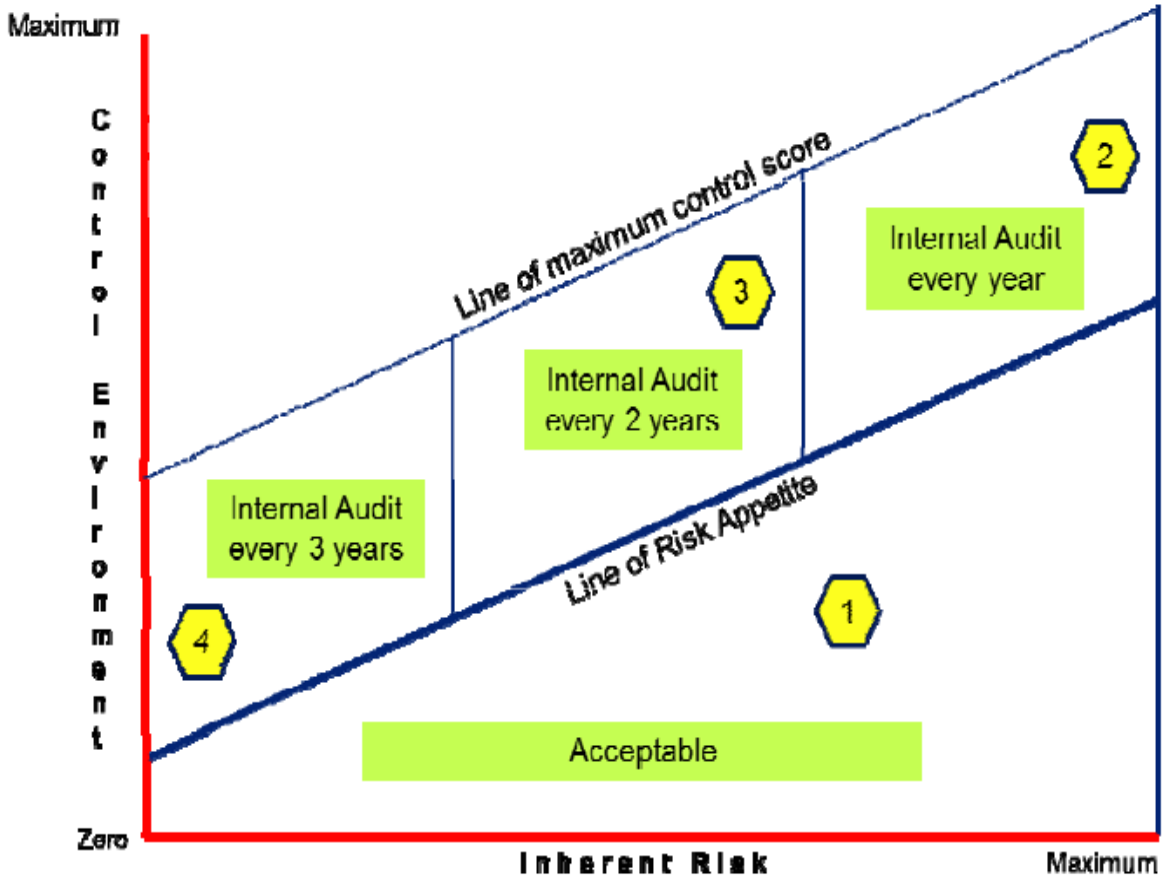
# Preliminary Risk Assessment & Control Environment Rating Matrix


**Control Environment Rating**

| | Insignificant (1) | Minor (2) | Moderate (3) | Major (4) | Critical (5) |
|---|---|---|---|---|---|
| Almost missing (5) | 5 | 10 | 15 | 20 | 25 |
| Week (4) | 4 | 8 | 12 | 16 | 20 |
| Moderate (3) | 3 | 6 | 9 | 12 | 15 |
| Strong (2) | 2 | 4 | 6 | 8 | 10 |
| Very Strong (1) | 1 | 2 | 3 | 4 | 5 |

**Preliminary Risk Assessment**

# Developing of RBIAP




Frequency of Audit and its Selection

1. Within tolerance limit – No immediate focus required
2. Inherent risk is maximum & control score is also high – Audited every year
3. Inherent risk is moderate & control score is also moderate – Audited every 3 years
4. Inherent risk is low & control score is also low – Audited every 3 years

# 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

# Resources

# Resources used for preparation of this presentation

- Guide on Risk Based Internal Audit and Risk Based Internal Audit Plan issued by ICAI
- Standards on internal audit issued by ICAI
- https://global.theiia.org/standards-guidance/topics/documents/201501guidetorbia.pdf
- www.theiia.org

# Q & A Session

# Thank You

C.A. Milan Mody