Risk Based Approach to Internal Audit

Evolution | Process | Regulations

Rachana Daftary

21 May 2021

mazars

Contents

Introduction

WHAT IS RISK

Risk is defined by International Organization for Standardization as:

- *"**Uncertainty** is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood."*

- *"Risk is often characterized by reference to **potential events and consequences** or a combination of these."*

EMERGING RISKS GLOBALLY

Cyber and data security

Regulatory change and compliance

Digitalization, new technology and AI

Financial, capital and liquidity risks

Human capital and talent management

Disasters and crisis response

Macroeconomic and geopolitical uncertainty

Supply chains, outsourcing, and 'nth' party risk

Corporate governance and reporting

Communications, management and reputation

RISK BASED INTERNAL AUDIT

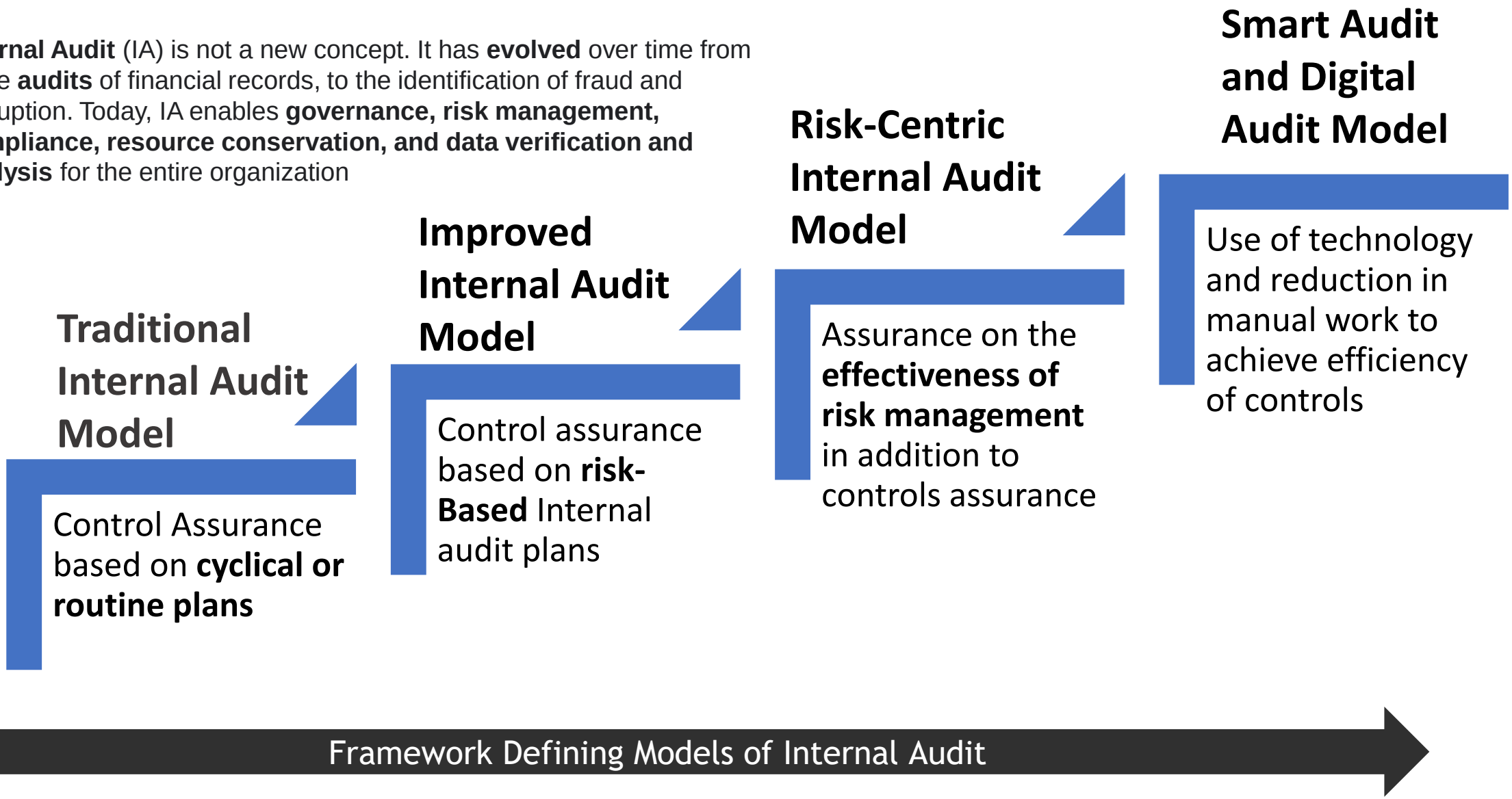
Risk-based internal audit (RBIA) is an internal methodology which is

- primarily focused on the **inherent risk** involved in the activities or system and

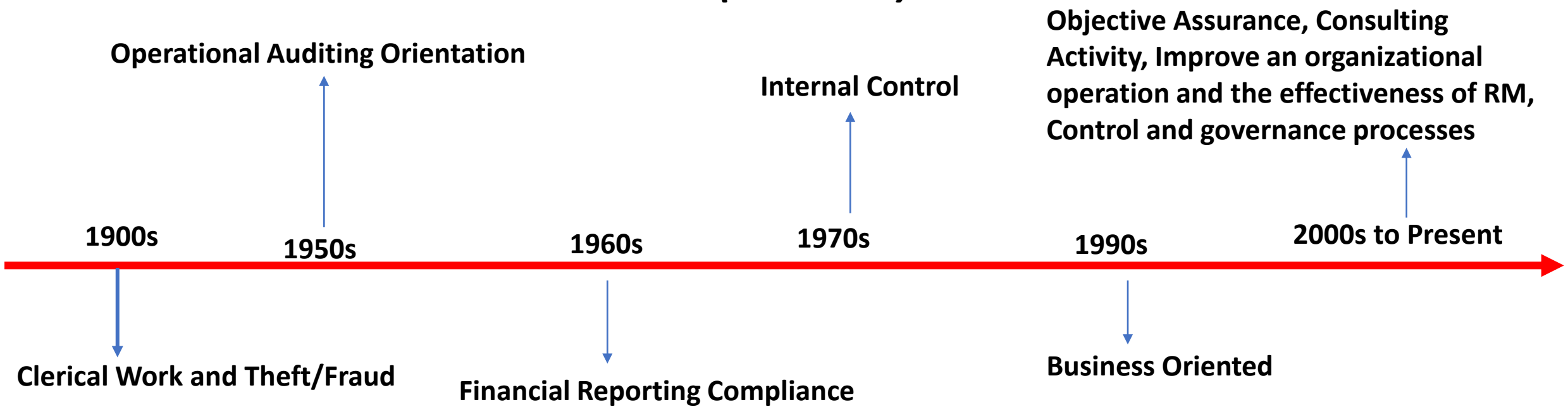
- provide **assurance** that risk is being managed by the management within the defined **risk appetite** level.

EVOLUTION OF INTERNAL AUDIT

Internal Audit (IA) is not a new concept. It has **evolved** over time from mere **audits** of financial records, to the identification of fraud and corruption. Today, IA enables **governance, risk management, compliance, resource conservation, and data verification and analysis** for the entire organization



EVOLUTION OF INTERNAL AUDIT *(CONT'D.)*



Key milestones:

IA set to emerge as key profession

1941- Formation of IIA
1947- Issued the statements of the responsibilities of the IA (Revised in 1957,1971,1976,1981, and 1990)

IA began as a profession

1968- Issued Code of Ethics
1972- Published the CBOK
1974- Created the professional Certification for IA
1976- Formation of the IIA research Foundation

Advances and strengthening of IA profession

1999- Issued Current Definition of IA
2000- Revised the Code of Ethics
2007- Issued a New IA Framework- the IPPF
2015- Issued a new enhancement of the IPPF
*IPPF is subject to update once in every 2 years

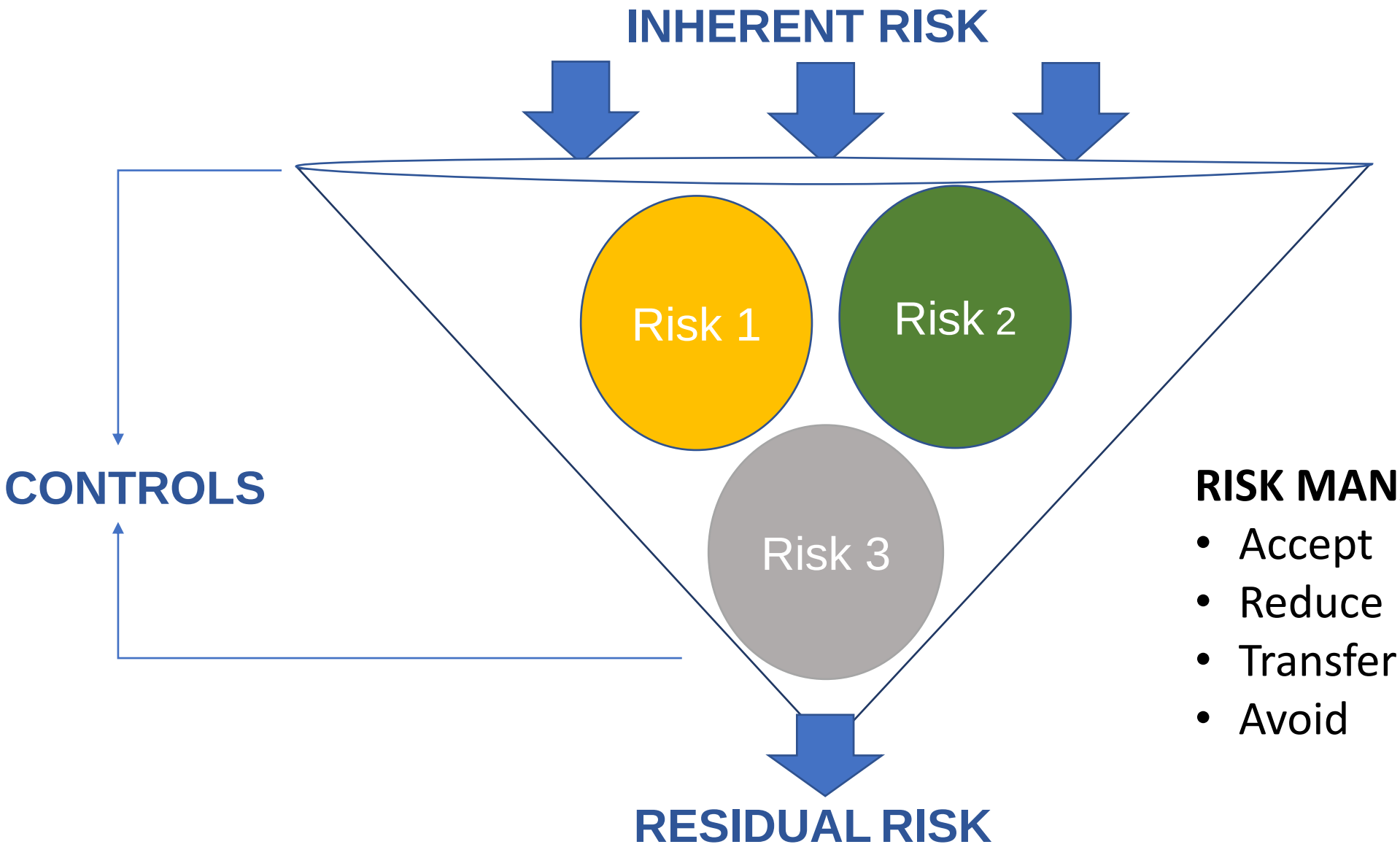
Regulatory landscape

REGULATORY FRAMEWORK

Statutes	Sections 134, 138, 177 of Companies Act 2013
	Securities and Exchange Board of India *(Listing Obligations and Disclosure Requirements)* Regulations, 2015
	CARO 2020- Internal Audit Systems
	RBI mandates for Banks, NBFCs, etc.

Risk Based Internal Audit

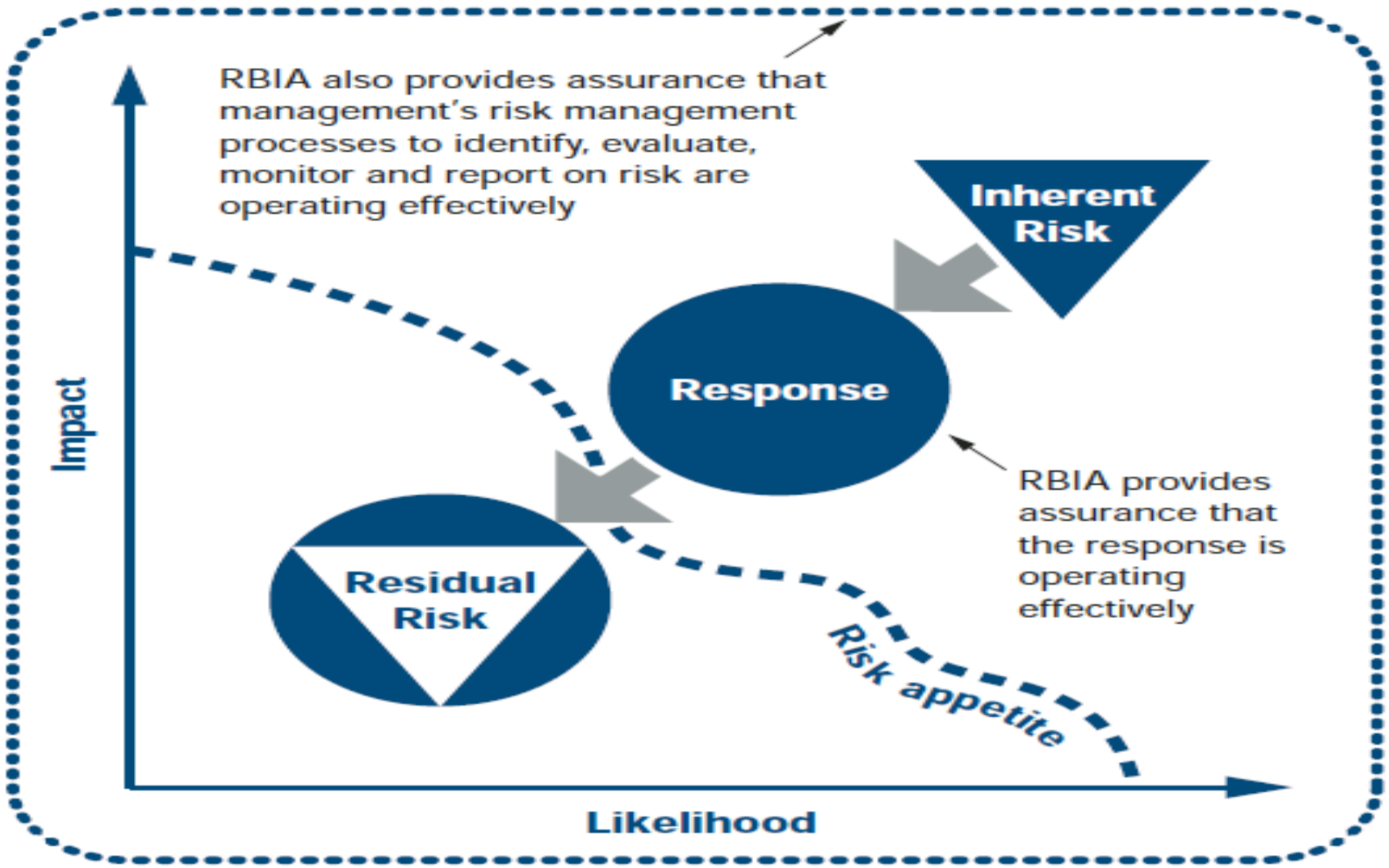
RISK, CONTROLS



RISK MANAGEMENT

- Accept
- Reduce
- Transfer
- Avoid

Assurance Provided by RBIA



CONTROL CHARACTERISTICS

- **Preventive :** Controls that **deters errors or mitigates risks** before they actually impact a business / process objective. Prevent controls are normally applied at a single transaction level. Examples include prior review and approval of transactions by a Manager, automated validity and edit checks.

- **Detective:** Controls that helps identify a risk that has **already impacted** a business /process objective. The purpose of detect controls is to identify on a timely basis errors that may have occurred during processing (*e.g., the errors that occur in spite of the company's prevent controls*). Example: Preparation of a Bank Reconciliation Statement helps identify incorrect transactions in the bank accounts

- **Directive:** Controls that increase the **possibility of a desirable behavior** to occur. Examples: training, incentive awards

- **Compensating:** Controls that **mitigate the effects of an error or misstatement** in the absence of a primary control. Examples: budget to actual analysis in lieu of detail transaction review, management review when segregation of duties is compromised

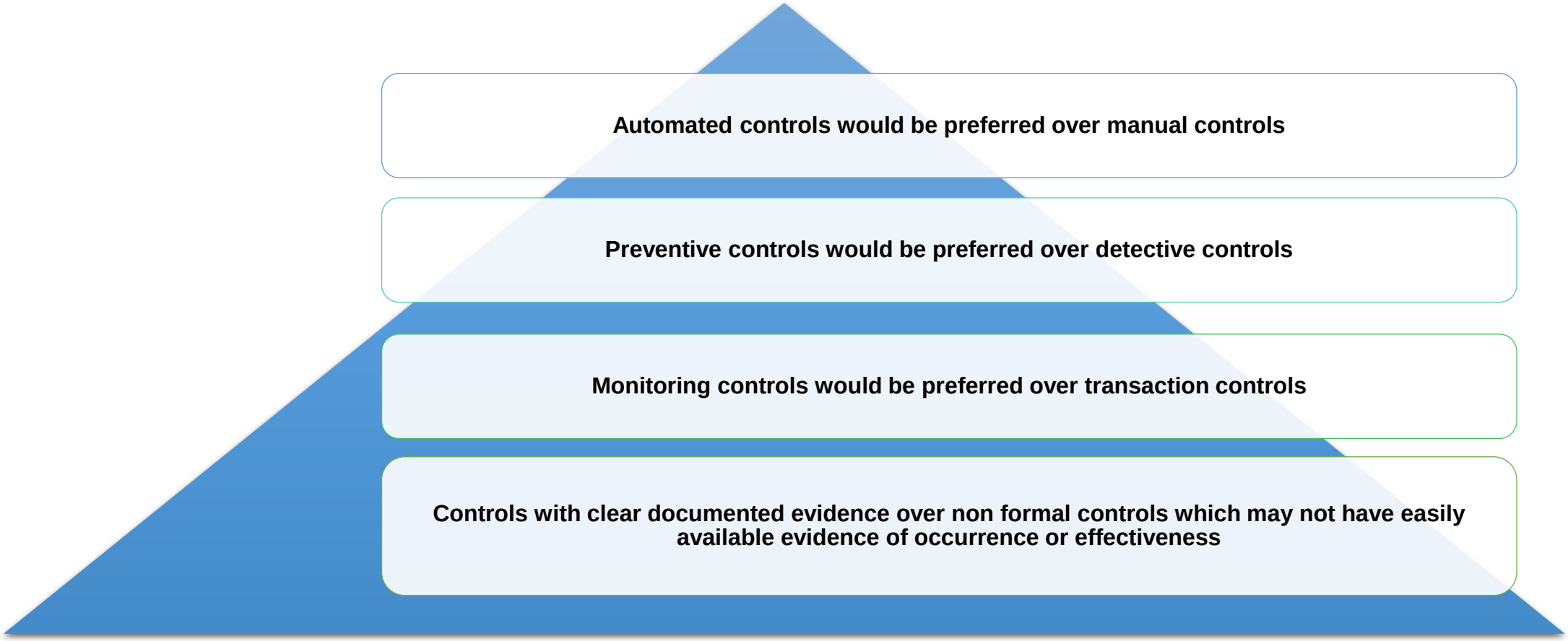
- **Manual control:** Controls that are **instituted outside any IT application**. Examples of controls performed manually include a review of Debtors analysis.

- **IT Dependent control**: Controls that are **manually performed, but require input based upon the results of computer-produced information**. Example: Management reviews monthly variance report and follows up on significant variances. Management relies on the computer-produced report to identify and generate variances.

- **Automated control:** Controls that are **embedded within the application and have no manual intervention** associated with it. Examples include edit checks, validations, calculations, interfaces, reporting and access. These are controls embedded within the application and have no manual intervention associated with it. 3 way check.

MULTIPLE CONTROLS MITIGATING THE SAME RISK

If there are multiple controls mitigating the same risk, the following aspects need to be considered to decide which control is to be relied on over the other.

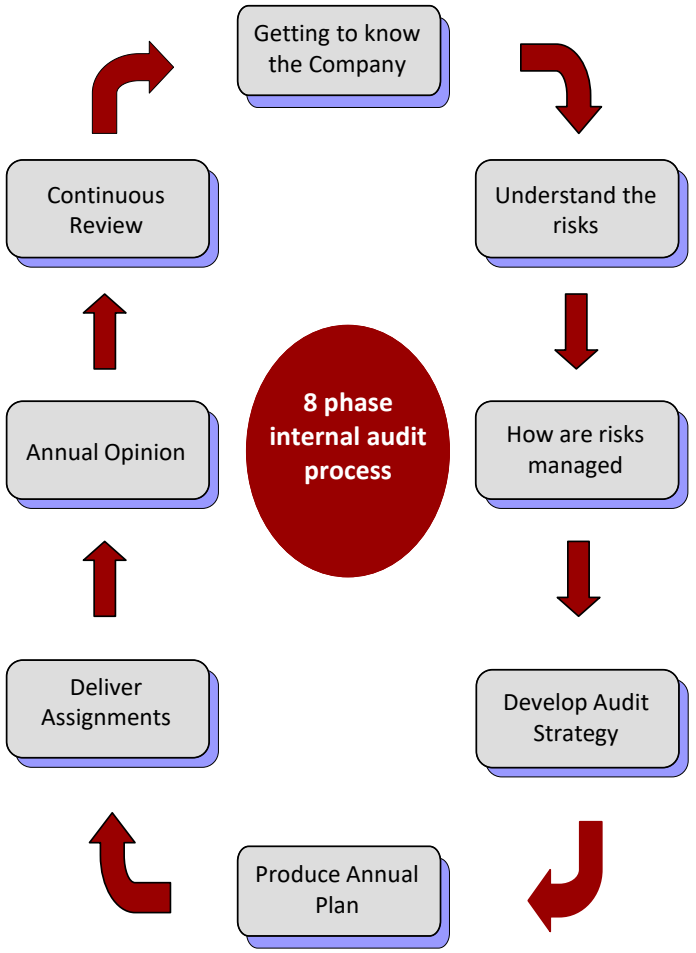


ADVANTAGES OF RISK BASED INTERNAL AUDIT

RBIA APPROACH

Methodology for RBIA is a risk based approach focusing on clients' strategic objectives and the risks and uncertainties which may affect their ability to achieve them.

Methodology should comply with the Institute of Chartered Accountants of India's internal audit standards & requirements.



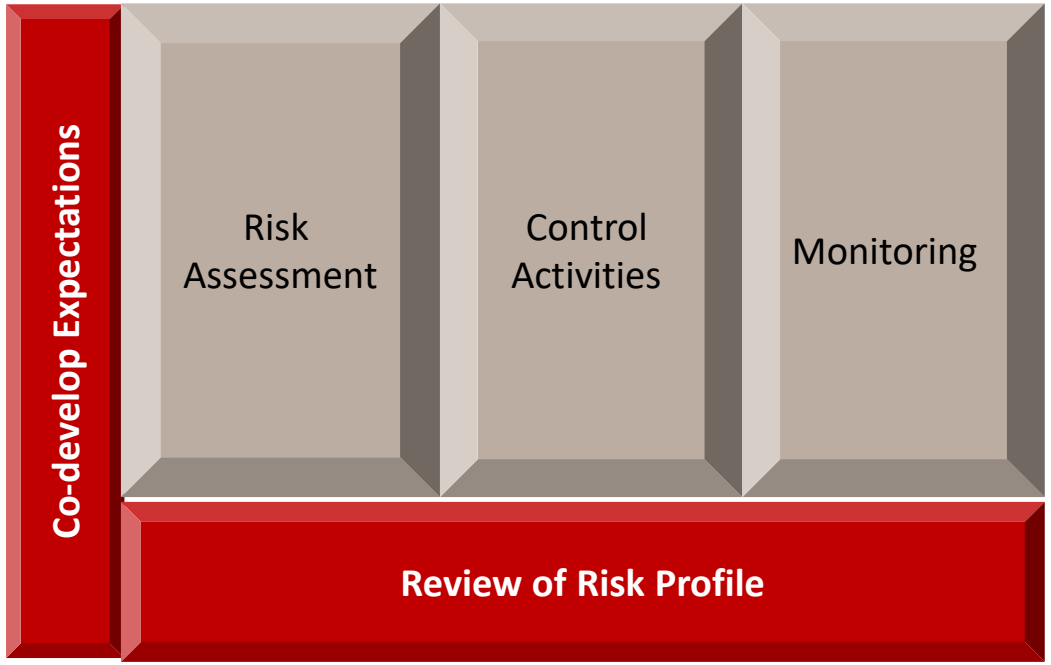
Key attributes of our methodology

Key attributes of the methodology are that it:

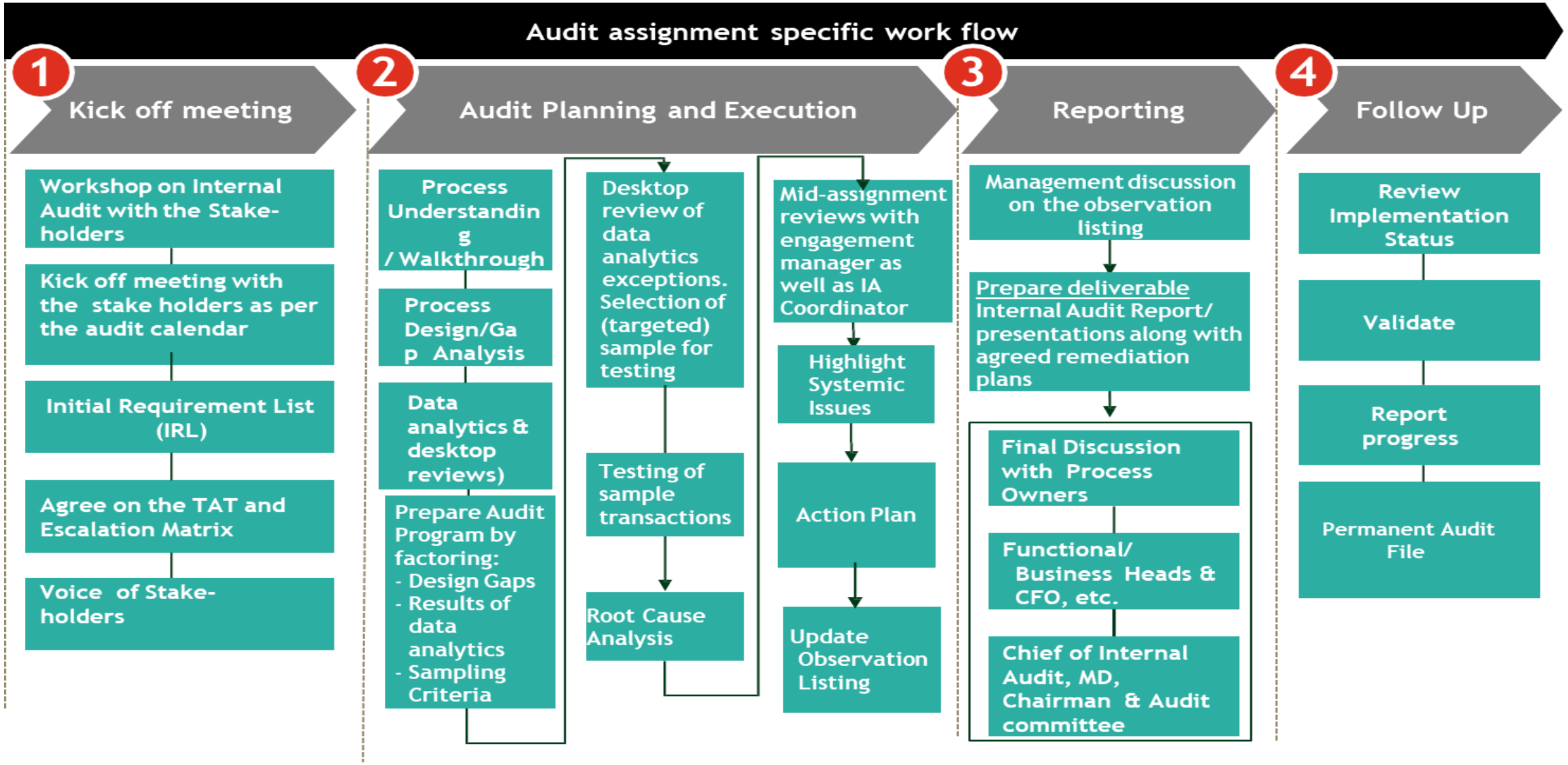
- is risk based *(arising out of discussions)* and focuses on Company's strategic objectives
- is designed to be scalable according to Company's needs
- Will be subject to successful external scrutiny
- encourages the use of specialists where appropriate
- Meets the definition of Internal Audit as issued by the ICAI

RBIA APPROACH *(CONT'D.)*

Internal Audit Service Delivery Framework should facilitate to comprehensively **evaluate and improve** the **effectiveness** of the Company's **internal controls system, risk management processes, and corporate governance**; its **focus**, **aligned** with organizations' **objectives** and strategies, is on effectual **management of key business risks**, and tangible and **sustainable improvement in business operations. Should enable business**



DETAILED INTERNAL AUDIT APPROACH



RISK CATEGORIZATION

STRATEGIC

- New Product Development
- Marketing Strategy
- Pricing Strategy

OPERATIONAL

- Technology & Infrastructure
- Cyber Security
- User Experience
- Cash flow management

COMPLIANCE

- Tax non compliances
- Data Privacy
- New statutes as applicable readiness- Labour code

REPORTING

- Inadequate cut off procedures
- Incorrect MIS

RATING CATEGORIZATION

Risk Factors	High	Moderate	Low
Potential Impact on P&L	More than INR _ million	INR _ million – _ million	Below INR _ million
COMPLIANCE			
Legal & Regulatory	Any failure to comply with legal/ regulatory requirements where there is prosecution and/ or significant penal and interest implications	Any failure to comply with legal/ regulatory requirements where penal and/ or interest implication is relatively high	Any failure to comply with legal/ regulatory requirements where penal and/or interest implication is low
OPERATIONAL			
Fraud Vulnerability	Any observation on probability of fraud	NA	NA
Policy definition and/ or documentation	Policy not defined and/ or documented OR Policy defined and documented with significant control gaps and evidence exists of financial loss *(annualized impact as per above scale)*	Undocumented processes are being followed; need documentation OR Policy documented with some control gaps and evidence exists of financial loss *(annualized impact as per above scale)*	Policy defined and documented but with minor procedural/ control gaps
Compliance to defined policies/ process	Significant level of non-compliance to critical policies/ processes ie those impacting revenues, costs, regulatory compliance, customer dissatisfaction, etc	Some non-compliance to critical policies/ processes ie those impacting revenues, costs, regulatory compliance, customer dissatisfaction, etc	Non-compliance to non-critical policies/ processes but which have a financial impact
Systems and Tools	Loss or exposure of confidential master or transaction data, System availability impacting business performance	Lack of adequate system validations/ access control/ controls which might lead to fraud	System bugs or functionality gaps impacting efficiency
Reputational impact	Any act resulting in reputation impact	NA	NA

Root cause definition

Process *(PR)*	When the process weakness/ control gap is as a result of inherent limitation of the business process
People *(PE)*	When the exception noted results from non adherence to laid down processes and procedures
IT	When the process weakness/ control gap is a result of inherent limitation of the information technology architecture supporting the business processes.
Best Practice *(BP)*	When there is possibility of improving the existing process as per the industry best practices

Process / IT Issue	High

Sales Order Approvals

Observation

Based on our discussions and walkthroughs, we observed :

- Absence of defined guidelines/ policy for providing guidance wrt sale order approvals considering amount, acceptable terms *(technical and commercial)* like liquidated damages *(LD),* taxation, advance, arbitration, jurisdiction, mark up, payment terms, etc.
- Absence of approval matrix for acceptance of LD or any such clauses which may not be in Company's best interests.

Risk/ Impact

- In the absence of guidelines and authority matrix there could be acceptance of sales order with terms detrimental to Company's interest.
- Acceptance of orders from customers with long outstanding, increasing the possibility of bad debts.

Root cause

- Absence of formalization of business processes.
- Absence of exploring and implementing automated functions and controls with SAP.

Recommendations

- Formulate a policy providing standard acceptable terms and defining authority matrix for review and acceptance of exceptional sales order terms.
- Configure SAP to mandate 3 layered approvals for orders with representatives from each Technical, financial, marketing teams with defined roles.

Management Response

- We agree to the recommendations, and a policy will be formulated providing std terms and defining authority matrix for acceptance of exceptions in SO terms.
- A 2 layer approval will be configured in SAP.

Timelines: 31- Dec-2020

Responsibility: Sales Head

Auditor's comments
The responses are satisfactory.

Audit Universe

OBJECTIVE, CRITERIA & RISK APPETITE

Objective, size, structure, culture, complexity,..

Criteria, maturity, priorities, regulatory framework, ..

Risk Appetite, risk taking ability

AUDIT UNIVERSE

Audit Universe comprises the Activities, Operations, Units etc., to be subjected to **audit** during the **planning** period;

The **Audit Universe** should be reviewed periodically and make amendments, wherever necessary;

In few cases the **Audit Universe** entirely changes depending on the scope given by the client.

RISK ASSESSMENT

Approach

Risk Identification

- Identify potential risks using desktop research and knowledge repository
- Discussion with Function Head and process owners
- Refine risk search based on feedback
- Risk evaluation and categorization
- Define mitigation plan

Risk Prioritization

- Assessment of identified risk
- Assessment of impact and likelihood
- Risk prioritization

RISKS ASSESSED

Output

- Risk Portfolio
- Risk Response

- **Prioritized Risks**
- **Risk Reporting Dashboards and Metrics**

Illustrative documents for risk assessment

Risk rating matrix – Impact

	Impact Areas	Parameters	Measurement Reference	Impact Rating			
				4 - Critical	3 - Significant	2 - Moderate	1 - Low
Impact	Financial	Impact on top line	INR	>10 Cr	>5Cr & <=10Cr	1Cr - 5Cr	<1Cr
		Impact on bottom line	INR	>2 Cr	>1Cr & <=2Cr	25 lakh - 1Cr	< 25 lakh
	Customer	Xxx	Xxx	>2%	>1% & <=2%	0.5% - 1%	<0.5%
		Xxx	Xxx	>2%	>1% & <=2%	0.5% - 1%	<0.5%
	Process	Compliance to legal and regulatory guidelines	Xxx	Xxx	Xxx	Xxx	Xxx
		Compliance to internal policies	Xxx	Xxx	Xxx	Xxx	Xxx
	People	Impact at Top / Senior management	Xxx	> 3	3	2	1
		Impact at Middle Management	xxx	> 15	>12 & <=15	10 - 12	<10

Risk category and classification

Risk Type	Definitions	Categories
Business and Strategic Risks	Risks related to business factors such as macro-economics and other external conditions, and the company's strategic response.	[B1] Business Strategy / Concentration [B2] Customer/Business Contracting [B3] Product Innovation/Global Contracting [B4] Competition [B5] External Factors
Financial Risks	Risks related to financial performance including future return on investment, financial statement integrity, and impact of divestitures and acquisitions.	[F1] Treasury/Capital Performance [F2] Financial Statement [F3] Transactional Activity [F4] Market / Credit Risk [F5] Interest Rates [F6] Economic Factors
Operational Risks	Risks of loss resulting from inadequate or failed internal processes, people, and systems. Most of these risks are managed by central corporate support units and executed locally by the Divisions.	[O1] IT Systems/Security [O2] Talent Management [O3] Legal [O4] Fraud [O5] Process Integrity/BCP [O6] Suppliers / Vendors
Regulatory Compliance Risks	Risks of a regulatory environment that are managed by each business line and affect the ability to meet earnings targets. In addition, business units are exposed to overall reputation in the marketplace.	[R1] Regulatory Oversight [R2] Privacy [R3] Geopolitical Risks affecting International Operations

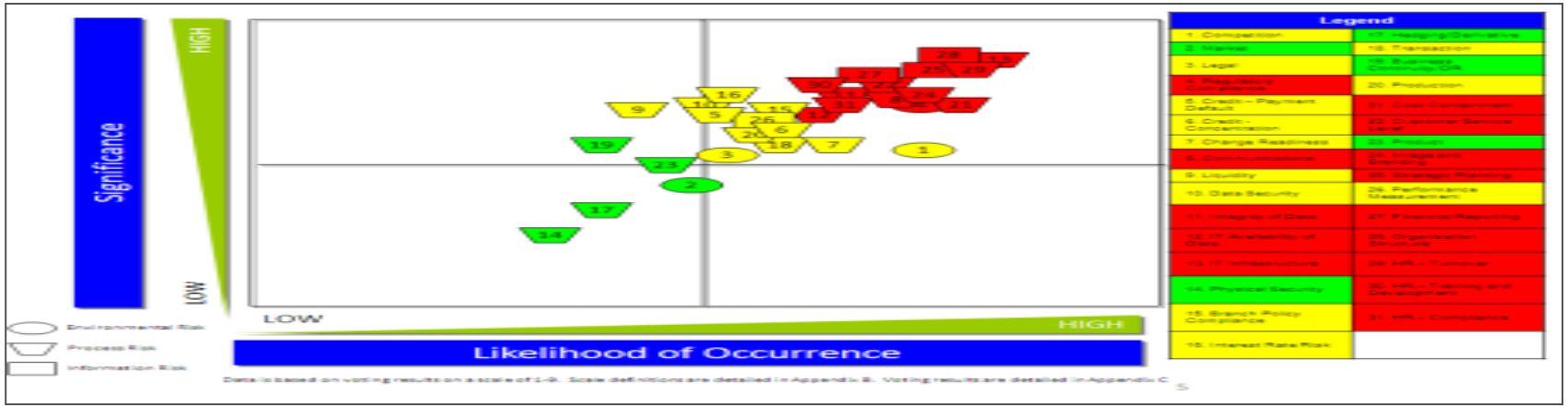
Risk rating matrix – Likelihood

		Parameters	Measurement Reference	Likelihood Rating			
				4 - Very Likely	3 - Likely	2 - Possible	1 - Unlikely
Likelihood		*For risks associated with transactional processes*					
	1	Probability	In 1 year	>=4%	>=2% &<4%	>=1% & <2%	<1%
		For risks associated with non-transactional internal events					
	2	Event occurrence	No of times since inception	> 5 times	3 - 5 times	2 times	< 2 times
		For external risk events – natural or manmade					
	3	Past occurrences	Time duration	Once a year or more	1 in 5 years	1 in 7 years	1 in 10 years

Illustrative documents for risk assessment

Risk prioritization rating

Overall Final Risk Rating				
Mitigation Effectiveness	**Inherent Risk Rating**			
	Green	**Yellow**	**Amber**	**Red**
Needs Improvement	Low	Moderate	High	Critical
Reasonably Adequate	Low	Moderate	Moderate	High
Effective	Low	Low	Low	Moderate



Illustrative approach for arriving at the Audit Universe

Areas are listed out along with processes, basis the risk assessment

Risk rating based on importance at Company level is assigned to processes

Defined no of areas are covered in a year, Mix of Business Unit coverage v/s Area/ process including theme based audits

Areas are shortlisted/ repeated each year based on the risk assessment

Internal Audit plan is provided and spread across 3-5 years

Indicative Audit Universe

Sr. No.	Audit Areas	Process	Risk Rating	Coverage				
				Year 1	Year 2	Year 3	Year 4	Year 5
1.1	Order to Cash	Marketing	Moderate	All Manufacturing units, Corporate office and Branches			All Manufacturing units, Corporate office and Branches	
1.2	Order to Cash	Inquiries Management	Moderate	All Manufacturing units, Corporate office and Branches			All Manufacturing units, Corporate office and Branches	
1.3	Order to Cash	Sales & Receivables	High	All Manufacturing units, Corporate office and Branches		All Manufacturing units, Corporate office and Branches		All Manufacturing units, Corporate office and Branches
2.1	Procurement to Pay	Raw Materials/ Trading Materials	High	All Manufacturing units, Corporate office and Branches	Follow up		All Manufacturing units, Corporate office and Branches	Follow up
2.2	Procurement to Pay	Engineering	High		All Manufacturing units	Follow up	All Manufacturing units	Follow up
2.3	Procurement to Pay	Spares	Moderate		All Manufacturing units	Follow up	All Manufacturing units	Follow up
2.4	Plant/ branch Operations	Production Planning	High	All Manufacturing units	Follow up	All Manufacturing units	Follow up	All Manufacturing units
2.5	Plant/ branch Operations	Contract Management	High	All Manufacturing units	Follow up	All Manufacturing units	Follow up	All Manufacturing units
2.6	Plant/ branch Operations	Quality Control	High	All Manufacturing units	Follow up	All Manufacturing units	Follow up	All Manufacturing units
2.7	Plant/ branch Operations	Costing	High	All Manufacturing units	Follow up	All Manufacturing units	Follow up	All Manufacturing units
2.8	Plant/ branch Operations	Manufacturing	High	All Manufacturing units	Follow up	All Manufacturing units	Follow up	All Manufacturing units
2.9	Plant/ branch Operations	Yield Analysis	High	All Manufacturing units	Follow up	All Manufacturing units	Follow up	All Manufacturing units
2.10	Plant/ branch Operations	Scrap management	High	All Manufacturing units	Follow up	All Manufacturing units	Follow up	All Manufacturing units
2.11	Plant/ branch Operations	Maintenance	High	All Manufacturing units	Follow up	All Manufacturing units	Follow up	All Manufacturing units
2.12	Plant/ branch Operations	Inventory Management	High	All Manufacturing units	Follow up	All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units
2.13	Plant/ branch Operations	Warehouse Management	High	All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches
2.14	Plant/ branch Operations	Logistics and Transportation	High	All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches

Indicative Audit Universe *(cont'd.)*

Sr. No.	Audit Areas	Process	Risk Rating	Coverage				
				Year 1	Year 2	Year 3	Year 4	Year 5
3.1	Accounts & Finance	Operating Expenses review	Moderate		All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up
3.2	Accounts & Finance	Financial closure & reporting	Moderate		All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up
3.3	Accounts & Finance	Treasury	Moderate		Corporate Office	Follow up	Corporate Office	Follow up
3.4	Accounts & Finance	Insurance	Moderate		Corporate Office	Follow up	Corporate Office	Follow up
3.5	Accounts & Finance	EXIM benefits	High		All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up
3.6	Accounts & Finance	Capex Management	Moderate		All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up
4.1	Human Resource & Payroll	Talent Acquisition	Moderate		All Manufacturing units, Corporate office and Branches		Follow up	
4.2	Human Resource & Payroll	Learning & Development	Moderate		All Manufacturing units, Corporate office and Branches			
4.3	Human Resource & Payroll	Compensation	Moderate		All Manufacturing units, Corporate office and Branches			
4.4	Human Resource & Payroll	Labour law compliances	High		All Manufacturing units, Corporate office and Branches			
4.5	Human Resource & Payroll	Payroll	Moderate		All Manufacturing units, Corporate office and Branches			
5.1	Compliances	Secretarial compliances	Moderate		Corporate Office	Follow up	Corporate Office	Follow up
5.2	Compliances	Direct Taxation	Moderate		All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up
5.3	Compliances	Indirect Taxation	Moderate		All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up
5.4	Compliances	Compliance tracking tool	High		All Manufacturing units, Corporate office and Branches	Follow up	All Manufacturing units, Corporate office and Branches	Follow up
5.5	Compliances	Related Party Transactions	High	Corporate Office	Corporate Office	Follow up	Corporate Office	Follow up
5.6	Compliances	Health, Safety & Environment *(HSE)*	High		All Manufacturing units	Follow up	All Manufacturing units	Follow up
6	Internal Financial Controls Testing will be undertaken each year, taking samples covering most business units, based on guidelines as per ICAI Guidance note.			✓	✓	✓	✓	✓

Audit Universe, some basics while developing it

Industry

Emerging risks

Control environment

Expectations

Recent developments

Quantitative & Qualitative

Striking a balance

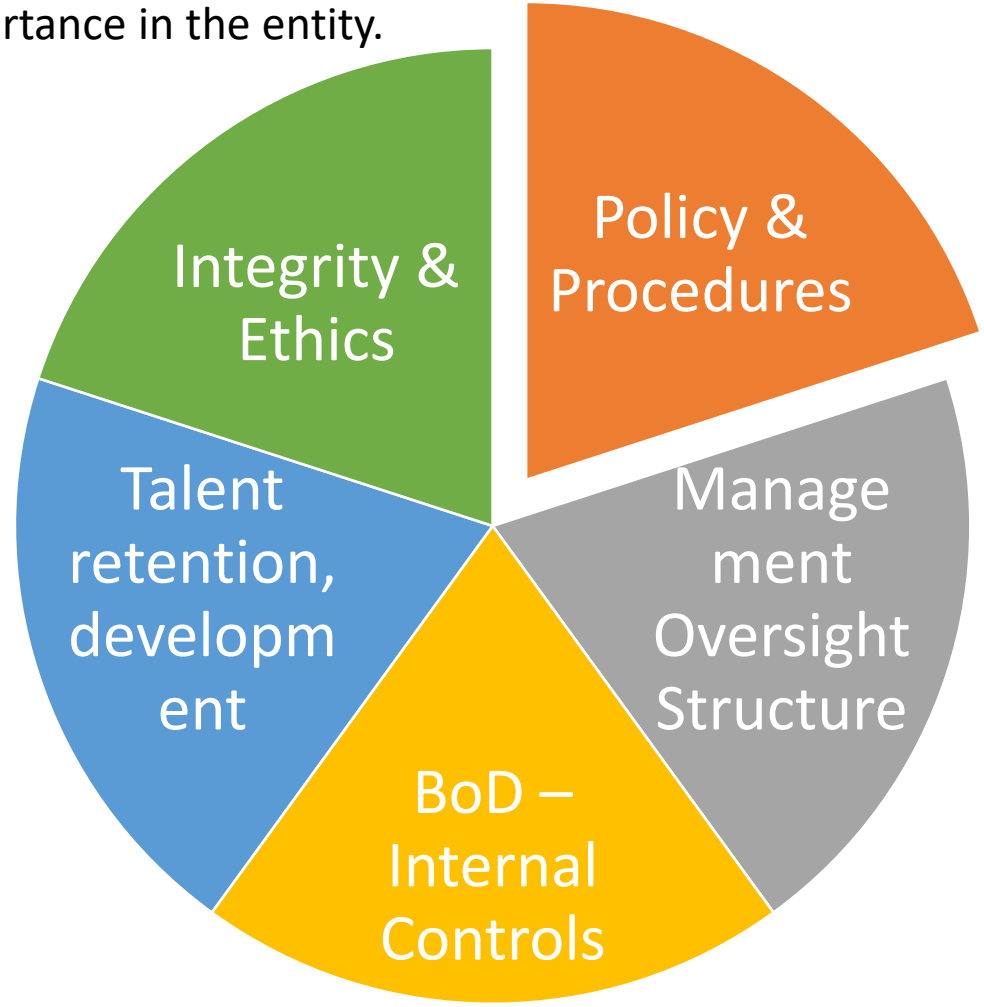
Engage

Not just books

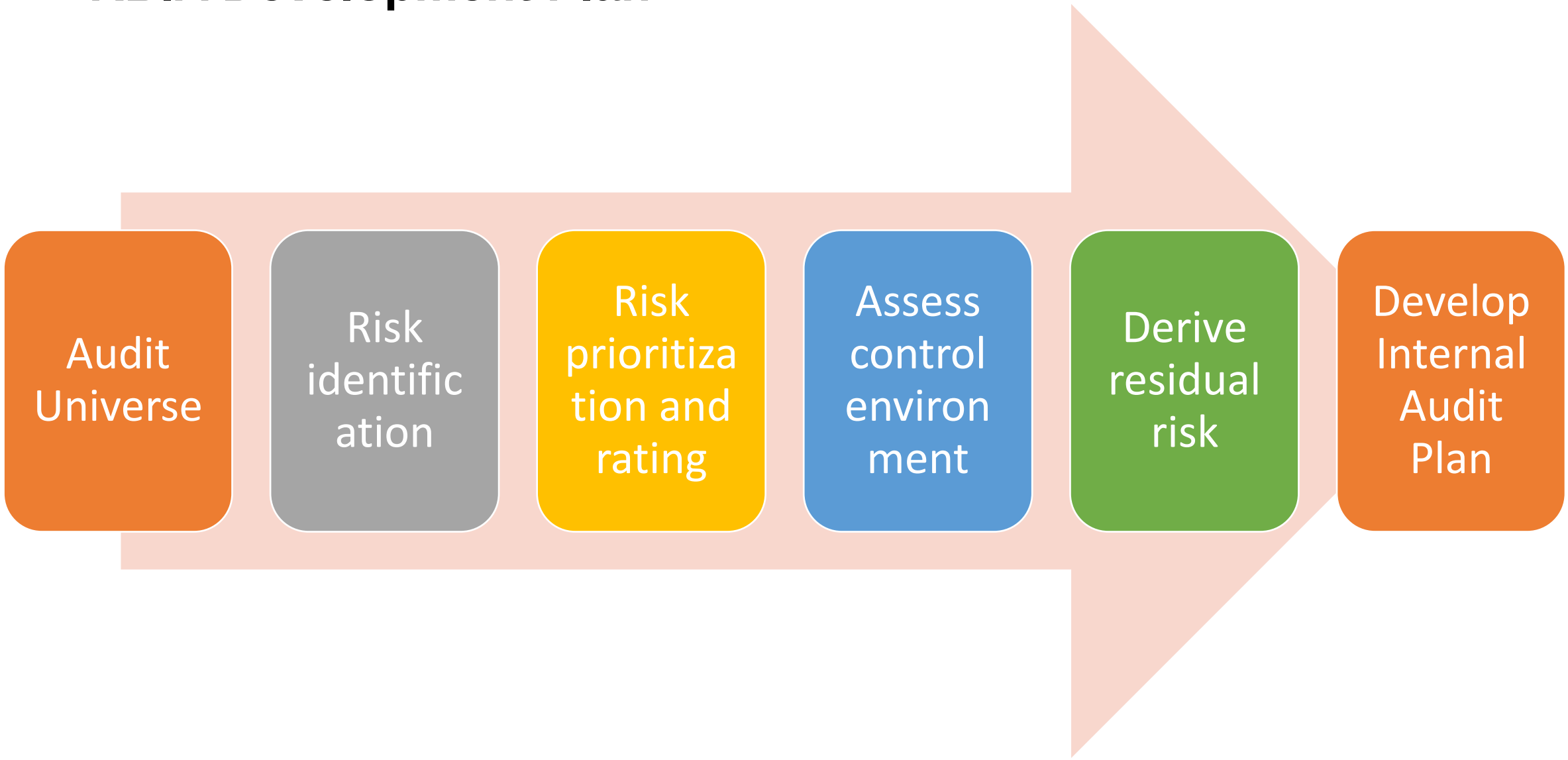
Justification for exclusions

Assessing control environment

Control Environment is overall attitude, awareness and actions of Directors and management regarding the internal control system and its importance in the entity.



RBIA Development Plan



RBIA Plan

Responsibility

- Chief Internal Auditor

Review Frequency

- Annual

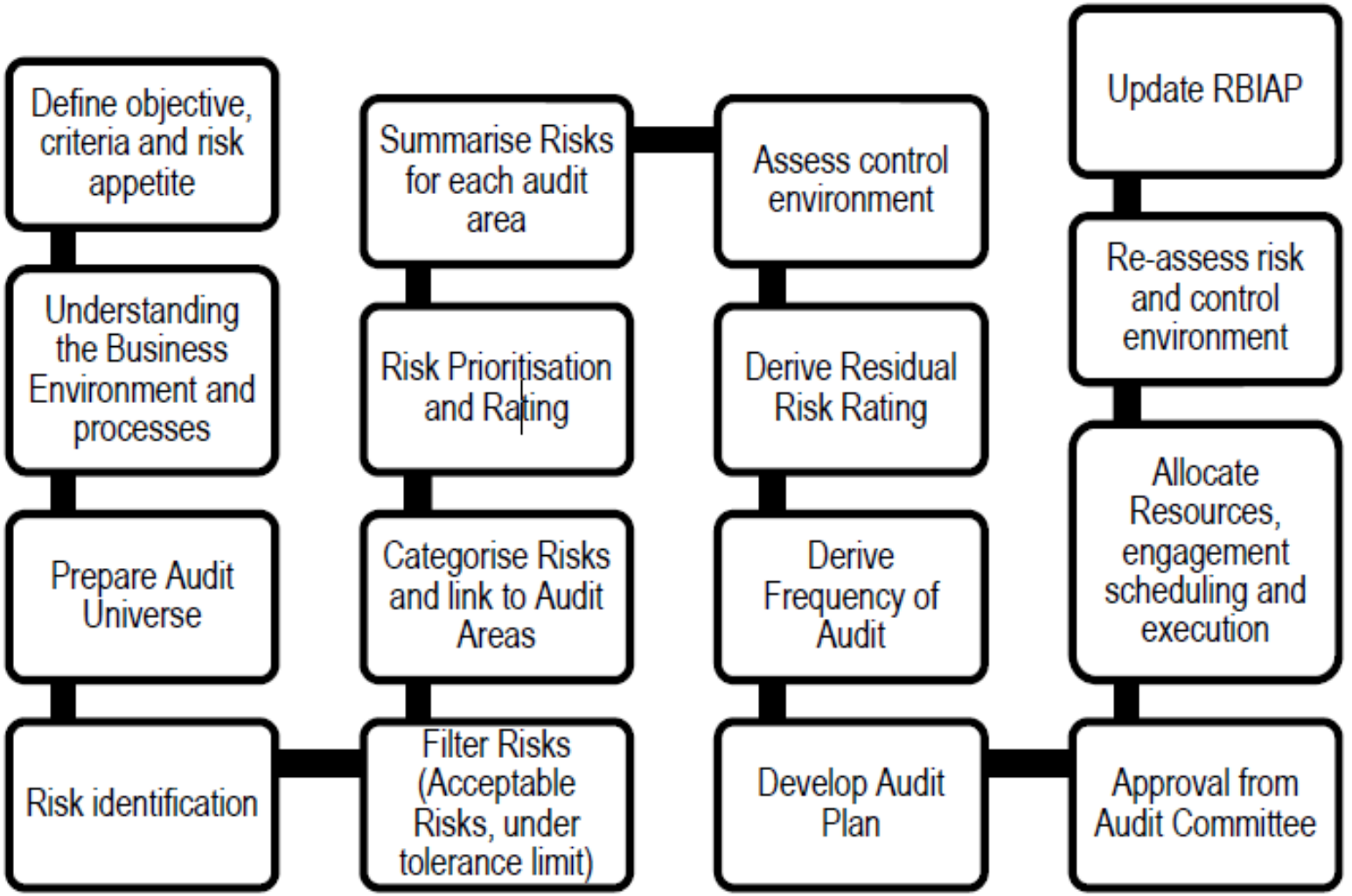
Approval

- Audit Committee/ Board of Directors

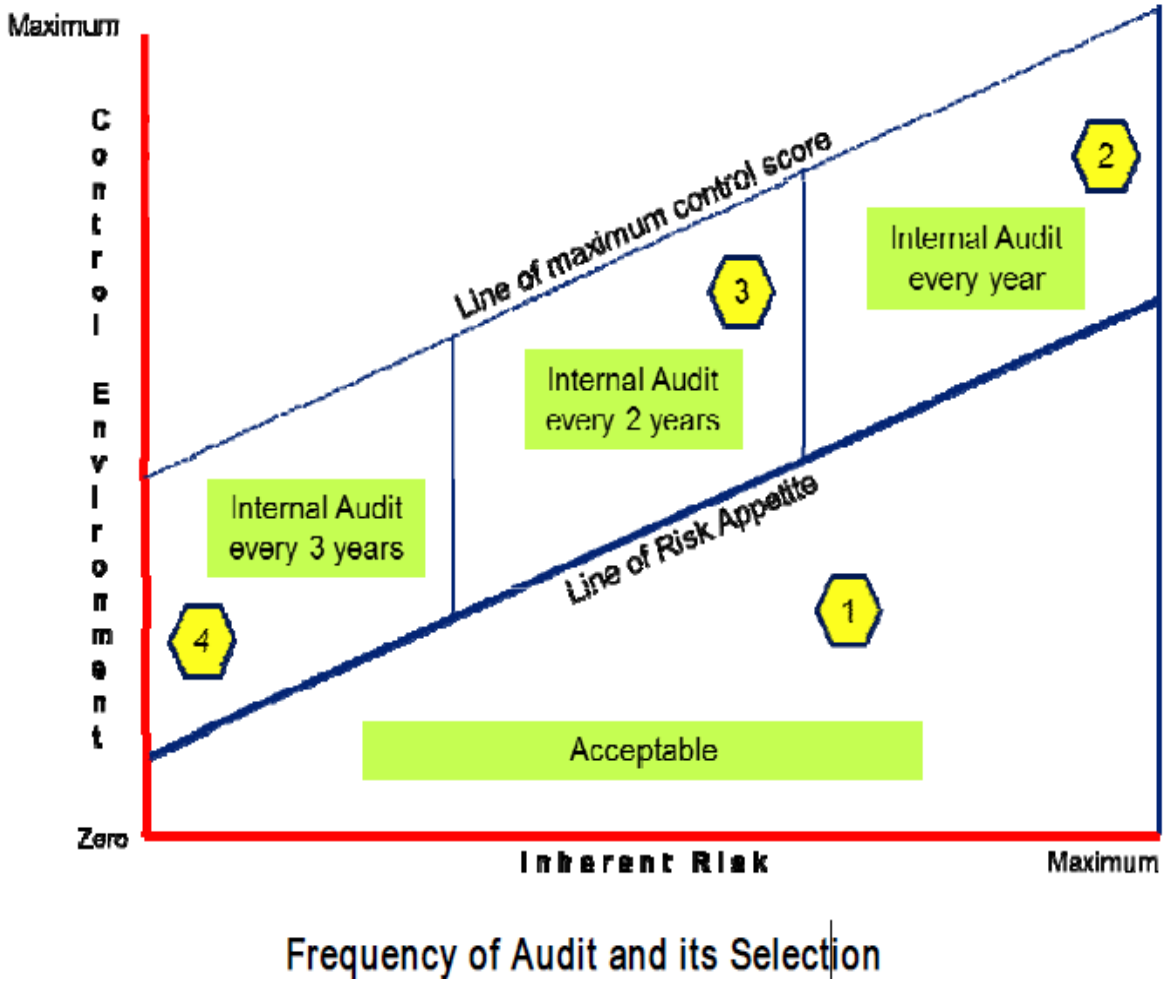
Considerations

- Risk Appetite
- Major risks
- Business Objectives,
- Business Environment,
- Management inputs,
- etc.

RBIA Plan, process



RBIA Plan Developed, Illustrative



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

Questions & Answers

Sources

www.theiia.org
www.icai.org- Guide on Risk Based Internal Audit and Risk Based Internal Audit Plan issued by ICAI

Contact

Rachana Daftary
Partner, GRRC
Mazars India LLP
E : rachana.daftary@mazars.in

REGISTERED OFFICE
Plant 13, Extension Office, Eastern Express Highway,
Pirojshanagar,
Vikhroli East, Mumbai – 400079

LinkedIn:
www.linkedin.com/company/mazars-in-india

Twitter:
www.twitter.com/MazarsGroup

Facebook:
www.facebook.com/MazarsGroup

Instagram:
www.instagram.com/MazarsGroup

*where permitted under applicable country laws.

www.mazars.co.in

Our Offices in India

MUMBAI
Plant 13, Extension Office, Eastern Express Highway, Pirojshanagar, Vikhroli East, Mumbai - 400079

AHMEDABAD
3rd Floor, Devpath Complex, Behind Lal Bungalow, Off C. G. Road, Ahmedabad - 380009

BENGALURU
2nd floor, 102 Gangadhar Chetty Road, Near Ulsoor Lake, Bangalore - 560042

CHENNAI
Alsa Mall, First floor, 149 Monteith Road, Egmore, Chennai - 600008

GURUGRAM
Mazars House, 421, Udyog Vihar, Phase IV, Gurgaon - 122016

KOLKATA
7th Floor, Infinity Benchmark, Sector V, Salt Lake, Kolkata - 700091

NEW DELHI
C-37, Inner Circle, Connaught Place, New Delhi - 110001

PUNE
3rd floor, Pro 1, Business centre, Plot 34-35, Senapati Bapat Road, Pune

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

mazars