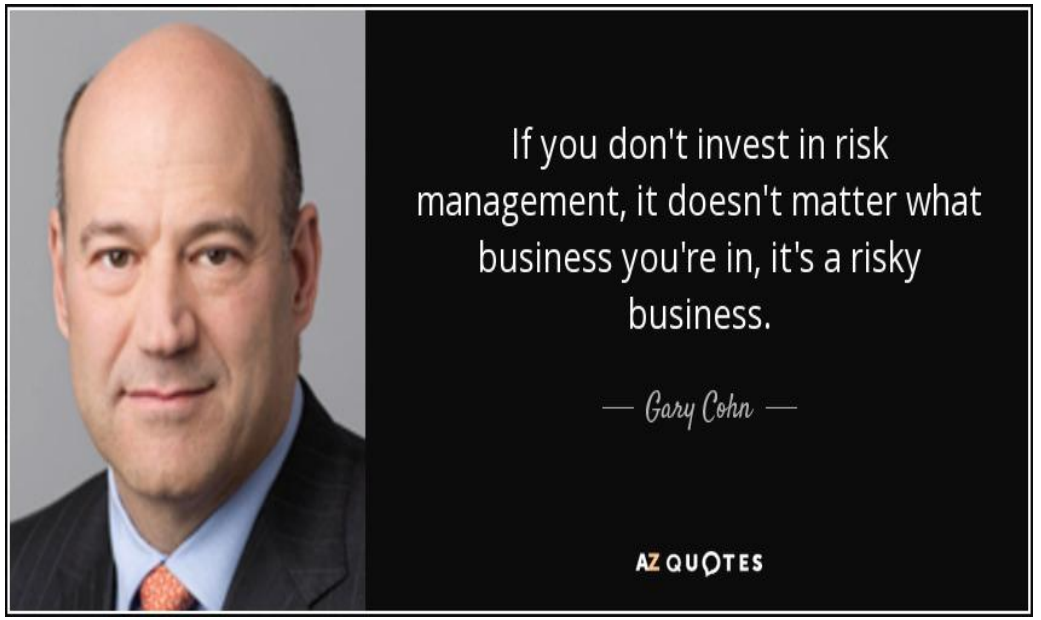
Risk Based Internal Audit – NBFC (RBI Directions)

Huzeifa Unwala, FCA CISA

October 7th, 2021

Topics

- HISTORY
- CONCEPTUAL FRAMEWORK
- IMPLEMENTATION STEPS



SYNOPSIS OF REGULATORY CIRCULARS AND GUIDELINES

December 27, 2002: Move towards Risk Based Supervision of Banks

- Banks should form a Task Force comprising senior executives-identify and address issues, action plan - report periodically to BOD and Top Management

December 27, 2002: Introduction of the New Basel Capital Accord

- Core principles and functions of Risk Based Internal Audit

February 01, 2005: Addressing gaps/ deficiencies to ensure that RBIA framework is effective

- Methodology for conducting the RBIA and policy to align the same with guidelines of RBI

August 25, 2016: Setting out scope and coverage of RBIA in commercial banks

- Permit banks to engage the service of its retired officials for assisting the internal audit.

January 07, 2021 Framework- Strengthening Governance arrangements

- To bring uniformity on Internal Audit functions

February 03, 2021 Extension of applicability of RBIA for NBFC and UCB (*)

- Threshold limit for applicability of RBIA:-
  - All deposit taking NBFCs
  - All Non-deposit taking NBFC with asset size of Rs 5000 Crore and above
  - All UCBs having asset size of Rs 500 crore and above.

(*) As per RBI Notification Dated June 11, 2021, w.r.t. circular Ref. No. DoS.CO.PPG/SEC.05/11.01.005/2020-21 dated February 03, 2021, it is stipulated that below mentioned entities shall put in place a RBIA framework by June 30, 2022, in accordance with the provisions of the aforesaid circular: -

- All deposit taking HFCs, irrespective of their size
- Non-deposit taking HFCs with asset size of ₹5,000 crore and above

TECHNOLOGY DISRUPTION IN FINANCIAL SERVICES SPACE

During the recent times, NBFCs are adopting business and operational models powered by technologies that helps in providing customized solutions, lower cost and increase in customer base. Technology has triggered need for Robust Risk Based Internal Audit in NBFCs as nature and type of risk have changed drastically. Technology disruption in NBFCs is due to the following key models across the value chain: -

Video KYC	Faster Loan Processing	Online Loan Bazaar	Automated Underwriting	Work From Home During Covid-19 Pandemic etc

LendingKart | SHIKSHA FINANCE | INCRED | Capital Float | KredX

BACKGROUND

- Uniformity in auditing approach for all supervised entities
- Transition from transactional auditing to Risk, Materiality and Inherency focused approach
- Alignment to global best practices on code of conduct – independence, rotation, competence, etc

Circular Roadmap

ROADMAP OF RBI CIRCULAR DATED FEBRUARY 03, 2021

APPLICABILITY	TIMELINESS	SMOOTH TRANSITIONING	COMMITTEE	REPORTING
NBFCs: - • All the Non-deposit taking NBFCs with asset size of Rs. 5,000 Crores and above, • All deposit-taking NBFCs irrespective of their Asset size and **UCBs: -** • All primary UCBs with the asset size of Rs.500 Crores and above **HFCs: -** • All deposit taking HFCs, irrespective of their size • Non-deposit taking HFCs with asset size of ₹5,000 crore and above	• **NBFCs** and **Urban Co-operative Banks** indicated in the directive shall implement the RBIA framework by **March 31, 2022** • **HFCs** indicated in the directive shall implement the RBIA framework by **June 30, 2022**	In order to ensure a smooth transition from the existing system of internal audit to RBIA, RBI has asked the concerned Entities to: - • Constitute a committee of senior executives with the responsibility of formulating a suitable action plan and asked the committee to address transitional and change management issues and • Should report the progress periodically to the board and senior management and implement the framework by March 31st, 2022	Constitute a committee of senior executive with Responsibility to formulate Action Plan	Periodical report to the Board and Senior management

KEY ELEMENTS OF RBIA AS RECOMMENDED BY RBI

WHAT IS RISK BASED INTERNAL AUDIT SYSTEM (RBI)?

As per RBI circular an effective Risk-Based Internal Audit (RBIA) is an audit methodology that links an organization's overall risk management framework and provides an assurance to the Board of Directors and the Senior Management on the quality and effectiveness of the organization's internal controls, risk management and governance related systems and processes

- A contemporary internal audit function plays a crucial role in evaluating a bank's internal control, risk management, governance systems and processes (in the context of both current and potential future risks) – areas in which the Boards and regulatory authorities have a keen interest.
- Further, internal auditors use risk-based approaches to determine their respective work plans and actions. The internal audit function should develop an independent and informed view of the risks faced by the bank based on their access to all bank records and data, their enquiries, and their professional competence.
- The head of internal audit is responsible for establishing an annual internal audit plan that can be part of a multi-year plan. The plan should be based on a robust risk assessment (including input from senior management and the board) and should be updated at least annually (or more frequently to enable an ongoing real-time evaluation of where significant risks lie).
- The board's approval of the audit plan implies that an appropriate budget will be available to support the internal audit function's activities. The budget should be sufficiently flexible to adapt to variations in the internal audit plan in response to changes in the bank's risk profile.

RBIA – Roles & Responsibilities as per RBI Direction

Board& AC

- Oversee RBIA
- Approve RBIA Policy
- RBIA Policy to clearly demarcate Purpose, Authority, Responsibility of IA & RM, etc
- Approve Annual Plan based on direction of Risk, as consistent with entity's goals
- Risk Assessment once a year
- Performance review of RBIA
- AC to formulate QAIP
- Promote use of new audit tools/ new technologies for reducing manual monitoring

Senior Management

- Adhere & implement RBIA policy
- Develop effective internal control function/ systems
- Ensure appropriate action is taken on internal audit findings within given timelines
- Present consolidated position of major risks faced by the organisation atleast annually to ACB/ Board, based on inputs from all forms of audit

IA

- Recommend to improve governance process on business decision making, risk management and control; promote appropriate ethics and values within organization, ensure effective performance management and staff accountability, etc

KEY ELEMENTS OF THE RBIA AS RECOMMENDED BY RBI

1	The internal audit shall undertake an independent risk assessment for the purpose of formulating a risk-based audit plan. This risk assessment would cover risks at various levels/areas (corporate and branch, the portfolio and individual transactions, etc.) as also the associated processes. The risk assessment in the internal audit department should be used for focusing on the material risk areas and prioritizing the audit work.
2	The risk assessment process should, inter-alia, include identification of inherent business risks in various activities undertaken, evaluation of the effectiveness of the control systems for monitoring the inherent risks of the business activities ('Control risk') and drawing-up a risk-matrix for both the factors viz., inherent business risks and control risks.
3	The basis for determining the level (high, medium, low) and trend (increasing, stable, decreasing) of inherent business risks and control risks should be clearly spelt out.
4	The risk assessment may make use of both quantitative and qualitative approaches. While the quantum of credit, market, and operational risks could largely be determined by quantitative assessment, the qualitative approach may be adopted for assessing the quality of overall governance and controls in various business activities.

KEY ELEMENTS OF THE RBIA AS RECOMMENDED BY RBI

5	The risk assessment methodology should include, inter-alia, parameters such as: - (a) Previous internal audit reports and compliance; (b) Proposed changes in business lines or change in focus; (c) Significant change in management / key personnel; (d) Results of regulatory examination report; (e) Reports of external auditors; (f) Industry trends and other environmental factors; (g) Time elapsed since last audit; (h) Volume of business and complexity of activities; (i) Substantial performance variations from the budget; and (j) Business strategy of the entity vis-à-vis the risk appetite and adequacy of control.
6	For the risk assessment to be accurate, it will be necessary to have proper MIS and data integrity arrangements. The internal audit function should be kept informed of all developments, such as introducing new products, changes in reporting lines, changes in accounting practices/policies, etc. The risk assessment should invariably be undertaken on a yearly basis. The assessment should also be periodically updated to consider changes in business environment, activities and work processes, etc.

KEY ELEMENTS OF THE RBIA AS RECOMMENDED BY RBI

7	The SEs may prepare a Risk Audit Matrix based on the magnitude and frequency of risk. The Audit Plan should prioritize audit work to give greater attention to the areas of: - (a) High magnitude and high frequency (b) High magnitude and medium frequency (c) High magnitude and low frequency (d) Medium magnitude and high frequency (e) Medium magnitude and medium frequency (f) Low magnitude and high frequency
8	The scope of the audit and resource allocation should be sufficient to achieve the objectives of the audit assignment. The precise scope of RBIA must be determined by each SE for low, medium, high, very high and extremely high-risk areas. The scope of internal audit should also include system and process audits in respect of all critical processes. The findings of such audits should also be placed before the IT Committee of the Board.
9	The internal audit report should be based on appropriate analysis and evaluation. It should bring out adequate, reliable, relevant and useful information to support the observations and conclusions. It should cover the objectives, scope, and results of the audit assignment and make appropriate recommendations and/or action plans.

KEY ELEMENTS OF THE RBIA AS RECOMMENDED BY RBI

10	All the pending high and medium risk paras and persisting irregularities should be reported to the ACB/Board in order to highlight key areas in which risk mitigation has not been undertaken despite risk identification.
11	The internal audit function should have a system to monitor compliance with the observations made by internal audit. Status of compliance should be an integral part of reporting to the ACB/Board.
12	The internal audit function shall not be outsourced. However, where required, experts, including former employees can be hired on a contractual basis subject to the ACB/Board being assured that such expertise does not exist within the audit function of the SE. Any conflict of interest in such matters shall be recognized and effectively addressed. Ownership of audit reports in all cases shall rest with regular functionaries of the internal audit function.

IMPLEMENTATION OF RBIA

REGULATORY EXPECTATIONS ON COMPETENCE & SKILLS OF IA FUNCTION

The desired areas of knowledge and experience include:-

a) Banking Operations
b) Accounting
c) Information technology
d) Data analytics
e) Forensic investigation, among others

HIA – Senior, independent, full access, ability to form opinions on other functions, reasonably long tenure as HIA, etc

KEY ACTIONABLE FOR IMPLEMENTING RBI CIRCULAR ON RBIA

STEP I: CREATE GOVERNANCE & FRAMEWORK

- RBI circular on RBIA should be placed before the Board in its next meeting. The implementation of these guidelines as per timeline specified should be done under the oversight of the Board
- Constitute a committee of senior executives with the responsibility of formulating a suitable action plan for implementation of RBIA
- The committee should address transitional and change management issues and should report progress periodically to the Board and Senior Management.
- Formulate and adopt board approved Risk Based Internal Audit (RBIA) policy. The policy should include: -
  - ✓ Purpose, authority, and responsibility of the internal audit activity,
  - ✓ Clear demarcation of the role and expectations from Risk Management Function and Risk Based Internal Audit Function.
  - ✓ The policy should be consistent with the size and nature of the business undertaken, the complexity of operations and should factor in the key attributes of internal audit function relating to independence, objectivity, professional ethics, accountability, etc.
  - ✓ The policy should also lay down the maximum time period beyond which even the low-risk business activities / locations would not remain excluded for audit.
- Ensure Implementation of the RBIA framework by March 31, 2022, in accordance with the Guidelines on Risk-Based Internal Audit from RBI

KEY ACTIONABLE FOR IMPLEMENTING RBI CIRCULAR ON RBIA

STEP II: IMPLEMENT FRAMEWORK – OPERATIONALIZING AND REPORTING

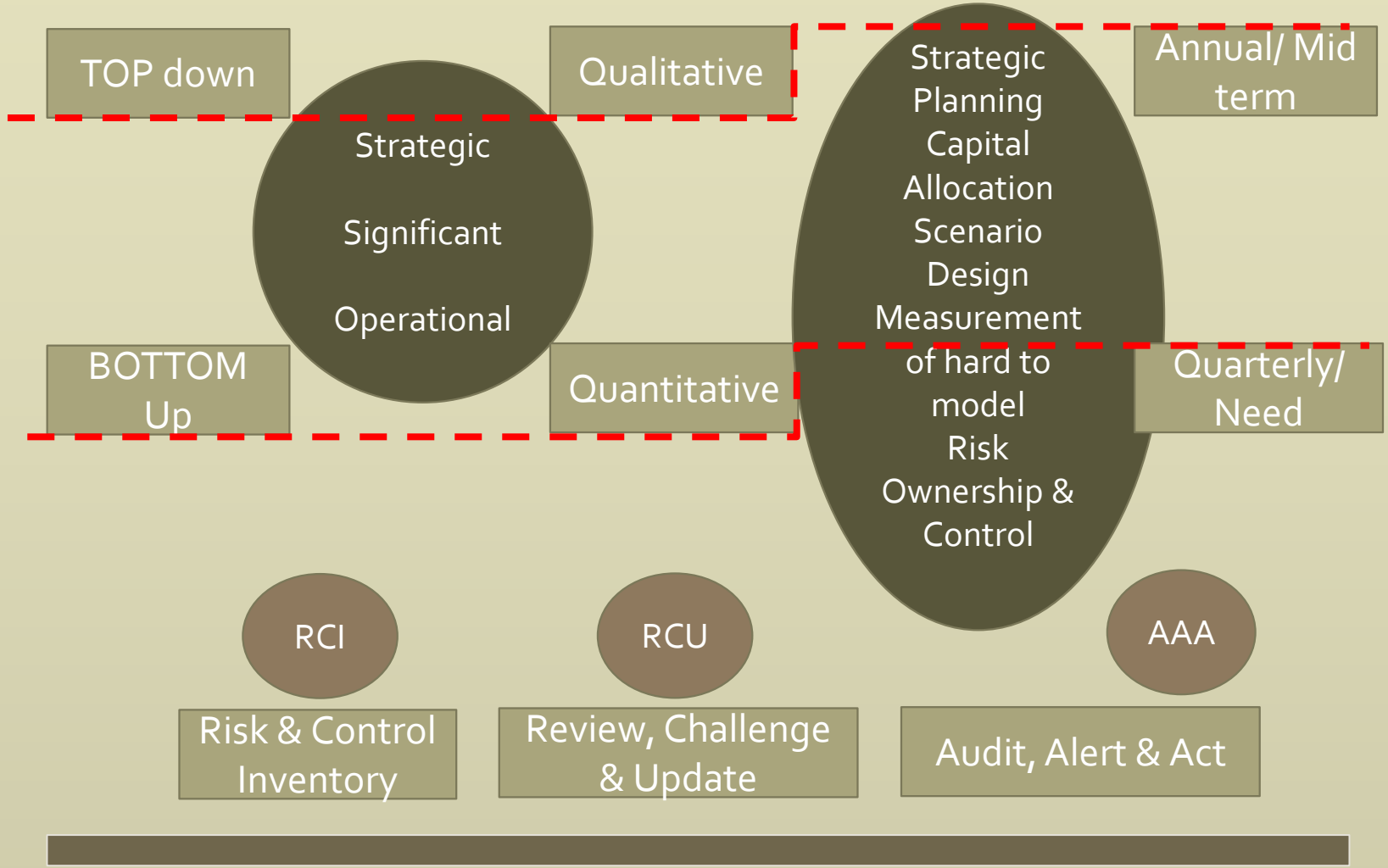
- Modify Terms of Reference of Audit Committee to include RBIA
- Appoint Internal Audit Head with sufficient authority, proper stature, independence, and ensure that there are adequate resources in the Internal Audit Team having professional competence. Allocate sufficient budget to the Internal Audit team.
- Internal Audit team should create audit universe and undertake an independent risk assessment for the purpose of formulating a risk-based audit plan considering inherent business risks emanating from an activity / location and the effectiveness of the control systems for monitoring such inherent risks.
- ACB/ Board shall approve RBIA plan to determine the priorities of the internal audit function based on the level and direction of risk, as consistent with the entity's goals.
- Carryout Risk Based Internal Audit (RBIA) having focus on the application and effectiveness of risk management procedures, risk assessment methodology a critical evaluation of the adequacy and effectiveness of the internal control systems. This risk assessment should cover risks at various levels/ areas (corporate and branch, the portfolio and individual transactions, etc.) as also the associated processes.
- Review RBIA policy periodically.

KEY ACTIONABLE FOR IMPLEMENTING RBI CIRCULAR ON RBIA

STEP II: IMPLEMENT FRAMEWORK– OPERATIONALIZING AND REPORTING (Cont'd)

- The ACB/ Board should review the performance of RBIA at least once in a year for adherence to the internal audit policy, objectives and expected outcomes.
- ACB/Board shall promote the use of new audit tools/ new technologies
- Internal Audit Team to present major risk faced by the organization at least annually to the ACB / Board: -
  - The internal audit function should assess and make appropriate recommendations to improve the governance processes on business decision making, risk management and control;
  - The internal audit function should provide vital assurance to the Board and its senior management regarding the quality and effectiveness of the entity's internal control, risk management and governance framework
- Strengthen MIS and IT

RISK IDENTIFICATION & ASSESSMENT



Risk Identification with respect to: -

- Entity
- Functions
- Processes
- Technology
- People
- Geography

Risk Identification Techniques, in general: -

- Risk climate surveys
- Developing Risk & Control Matrix
- Tracking risk events and documenting impacts/ causes
- Materiality assessment
- Risk focused meetings
- Research sharing amongst peers
- Product specific risk analysis or research
- Data aggregation & warehousing to build trends, outliers, exceptions, etc
- Self-assessments and measurements

INDEPENDENT RISK ASSESSMENT TEMPLATE BY IA – [ILLUSTRATIVE TEMPLATE/ANNUAL]

RBI Prescribes/ the risk assessment methodology should include, inter-alia, parameters such as: -

(a) Previous internal audit reports and compliance;
(b) Proposed changes in business lines or change in focus;
(c) Significant change in management / key personnel;
(d) Results of regulatory examination report;
(e) Reports of external auditors;
(f) Industry trends and other environmental factors;
(g) Time elapsed since last audit;
(h) Volume of business and complexity of activities;
(i) Substantial performance variations from the budget; and
(j) Business strategy of the entity vis-à-vis the risk appetite and adequacy of control.

NAME OF ENTITY		LOCATION	
Name of Unit		Materiality	
Risk Assessment Objective		Level of Risk (H/M/L)	
Major Risk Components/ Concerns	a) History of exceptions/ audit/ frauds b) Process/ Inherent c) Activities & Locations d) People e) Technology f) Major changes since previous review g) Performance h) Fraud indicators i) External factors j) Compliance amendments k) Third Parties l) Data analytics insights		
Unit Risk Profile		a)	Unit Risk Trend (>, <, =)
Unit Leve	a) Positive Factors	a)	Negative Factors
Risk Priorities			

Annual Risk Identification on two vectors: -

- Inherent Risk

- Control Risk

Inherent Risk

Inherent Business risks indicate the intrinsic risk in a particular area/activity of the Bank and could be grouped into low, medium and high categories depending on the severity of risk.

Control Risk

Control risks arise out of inadequate control systems, deficiencies/gaps or likely failures in the existing control processes, incidents pointing to gaps in implementation of control processes etc. The control risks could also be classified into low, medium and high categories.

ANNUAL PLAN – (ILLUSTRATIVE)

- Risks Not Subject to IA
- Skill Gap
- Extent of Testing
- Flexibility & Contingency

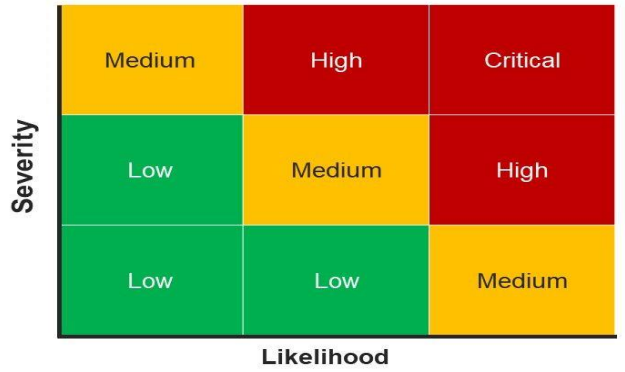
Audit Cycles	Risk Level	Frequency	Yr I	Yr II	Yr III
LENDING OPERATIONS					
Commercial Loans	M	2	X		X
Consumer Loans	M	2		X	
Real Estate Loans	M	2	X		X
Credit Administration	H	1	X	X	X
Secondary Marketing	L	3		X	
TREASURY MANAGEMENT					
Securities	M	2	X		X
Cash Management	L	3			X
Asset/Liquidity Management	M	2	X		X
Wire Transfer	H	1	X	X	X
Automated Clearing House	H	1	X	X	X
Borrowings and Repurchase Agreements	L	3		X	
ACCOUNTING AND FINANCIAL REPORTING					
General Accounting	M	2		X	X
Financial Reporting	M	2		X	
DEPOSIT OPERATIONS	M	2		X	
BRANCH OPERATIONS	M	2	X		X
BANK ADMINISTRATION					
Human Resources	M	2	X		X
Payroll	L	3		X	
Purchasing	L	3		X	
Insurance Coverage	M	2	X		X

High (H); Medium (M); Low (L)

Risk Audit Matrix: -

- Impact of Issue
- Probability of Occurrence
- Control Effectiveness Score

Risk Heat Map

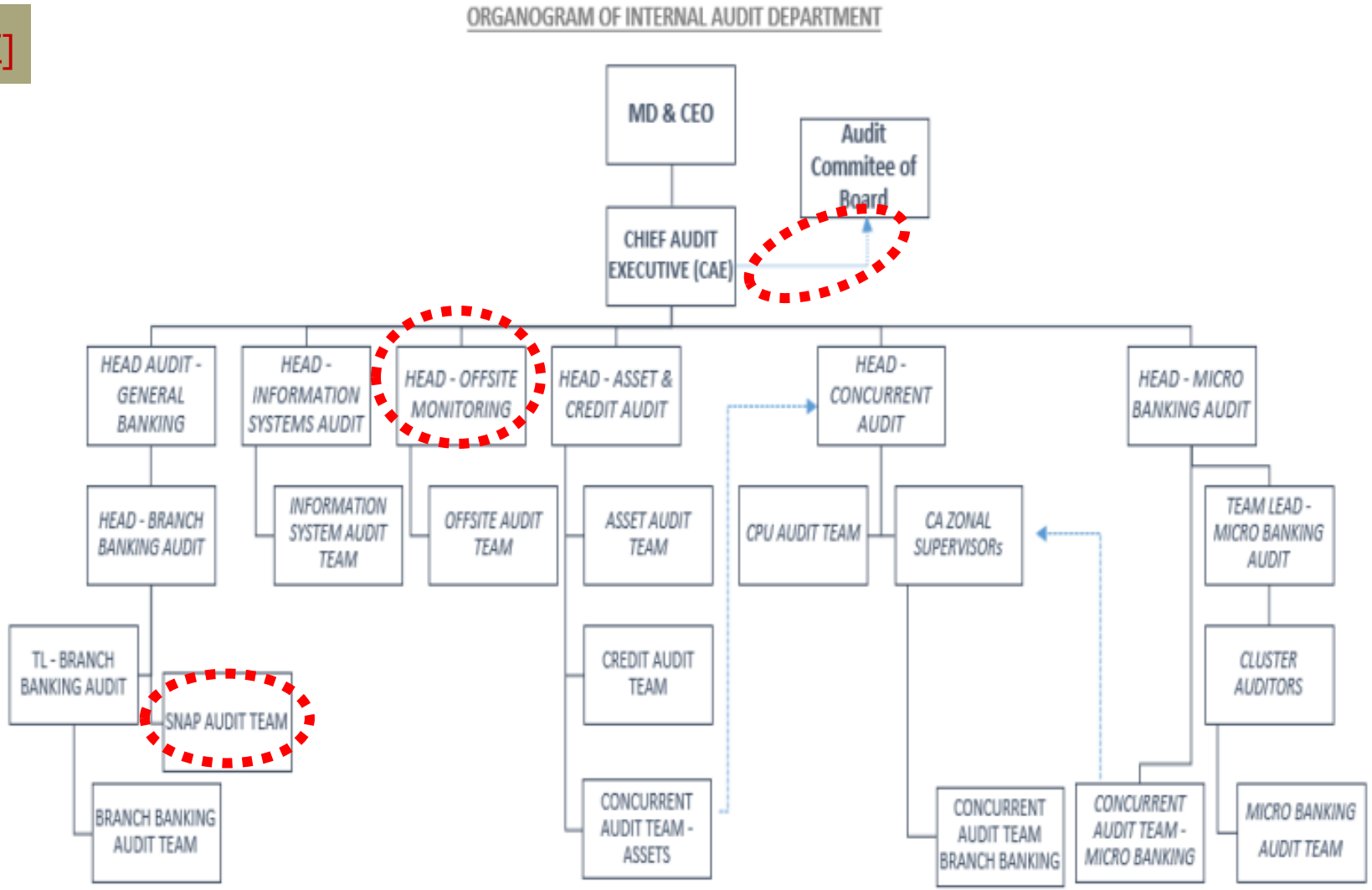


Control Effectiveness Map

Ratings	Control Scores	Audit Opinion	Control Risk
A	≥ 85	Effective	Low
B	≥ 75 < 85	Meets Requirement	Medium
C	≥ 70 < 75	Partially Effective	
D	≥ 65 < 70	Improvement Needed	High
E	< 65	Significant Improvement Needed	

CONTEMPORARY RBIA FUNCTION

[ILLUSTRATIVE]



1

Risk Profile of each Regulated Entity

- RBIA links SE risk profile to internal audit system
- RBIA introduces a risk scoring system
- Policy for RBIA

2

Function, Authority & Stature

- Authority is defined through a Charter
- Competence
- Rotation of Staff
- Reporting Line
- Remuneration
- Independence
- Performance evaluation
- Quality Assurance
- KPIs

3

Risk Assessment

- Corporate Level
- Branches
- Portfolio
- Off-site
- On-site
- After on-site
- Planning stage
- Execution stage
- Risk Assessment Methodology
- Risk Matrix
- Sampling to vary depending to risk profile
- Monitoring the Risk trend

RBIA – FUNCTIONAL BREAK DOWN

COMPONENT I	COMPONENT II	COMPONENT III	COMPONENT IV	COMPONENT V	COMPONENT VI	COMPONENT VII
Organization Structure and Independence	Strategy and Planning	People, knowledge and skills	Internal Audit Processes, Methodology and Resources	Other Assurance Providers	Reporting & communication	Systems & Information

RBIA - COMMUNICATIONS

- Risk focused Internal audit reports – ratings or subject matter opinions
- Fraud risk related – assessments, agreed upon procedures
- Risk & Controls Assessment of key accounting balances
- IA - Dashboard for continuous improvement activities
- Progress reporting on establishment of centers of excellence (automation)
- Key insights on emerging matters
- Self-assessment outcomes
- Third party risk assessments / outsourcing audits/ SSAE 18 attestations

IMPLEMENTATION CHALLENGES

- Awareness, knowledge & competencies
- Organizational alignment
- Budgeting & Resources
- Specialized people for risk identification at business/ risk unit level
- Suitable technology stack

RBIA – GOOD IS BETTER THAN PERFECT

IIA - IPPF 2120:-

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities."

Thank you

Huzeifa.unwala@jhsassociates.in