Author: Subhojit Shome | subhojit@vinodkothari.com
Date: July 13, 2023

Risk-based Internal Audit (RBIA)

Applicability and Implementation Aspects for NBFCs

Table of Contents

Introduction

On January 7, 2021, the RBI issued the circular - *RBIA Framework for Strengthening Governance Arrangements ('Circular on RBIA for Banks')* applicable to commercial, local area small finance and payment banks. Considering the increase in the size of the balance sheets of certain NBFCs and their financial interconnectedness, on February 3,2021, the RBI followed up the circular on RBIA for Banks with one for NBFCs ('*RBIA Circular*'), to increase focus on their risk management function. The requirements prescribed under the circular were to be implemented by March 31, 2022.

With the introduction of this Circular, there have been questions raised as to the type of NBFC that fell under the ambit of the RBIA Circular and in case they did fall under it, the changes that would be needed in their current internal audit practices so as to be compliant with the RBIA mandate.

We have already covered, at a broad level, the action points that arise for NBFCs as a result of the RBIA Circular. In this article, we focus specifically on the NBFCs that require to implement the RBIA framework and changes that are needed in their current internal audit practices.

Applicability

The said circular is applicable on the following types of NBFCs -

Type of NBFC	Applicability
Deposit taking NBFCs (NBFC-D)	Applicable
Non-Deposit taking NBFC (NBFC-ND):	
NBFC-ND with asset size less than or equal to ₹ 5000 crore	Not Applicable
NBFC-ND (incl. CICs) with asset size greater than ₹ 5000 crore	Applicable

Table 1: Applicability of the RBAI Circular to NBFCs.

HFCs brought within ambit of RBIA

There were questions raised by stakeholders whether Housing Finance Companies (HFC) also needed to perform risk-based internal audit and the RBI's response was in the affirmative vide its June 11, 2021, circular, wherein it clarified that -

> *On a review, it has been decided that the provisions of the aforesaid circular (circular dated 3rd February, 2021) shall be applicable to all deposit taking HFCs, irrespective of their size and non-deposit taking HFCs with asset size of ₹5,000 crore and above.*

Nature of RBIA

As per the RBIA Circular, historically, the internal audit system in NBFCs has generally been concentrating on transaction testing, testing of accuracy and reliability of accounting records and financial reports, adherence to legal and regulatory requirements, etc. However, in the changing scenario, such testing by itself might not be sufficient and the RBI has mandated NBFCs to adopt a framework that will include, in addition to selective transaction testing, an evaluation of the risk management systems and control procedures in various areas of operations.

Evolved Methodology for performing Internal Audit

The ICAI Guide on RBIA clarifies that RBIA is not different from internal audit. Compared with the traditional internal audit process, RBIA can be described as internal audit performed using a risk-based methodology. RBIA is based on the fact that it is the NBFC's management that is responsible for implementing enterprise-wide risk management processes and the internal auditor audits the risk management processes of the NBFC. In planning the audit and its coverage it relies ("if found reliable") on the management's assessment of risk. Hence audit effort is targeted at the areas that require most focus based on their risk assessments.

This approach - audit of risk management processes and not audit of risk - is based on the principle that management knows their business best and the auditor is the subject matter expert when it comes to internal control.

Part of Overall Risk Management

The RBIA Circular provides that the internal audit function continues to be an integral part of sound corporate governance and is considered as the third line of defence. The reference to lines of defence for risk management may be drawn from the RBIA circular for Banks[1], which provides as follows-

[1] ibid

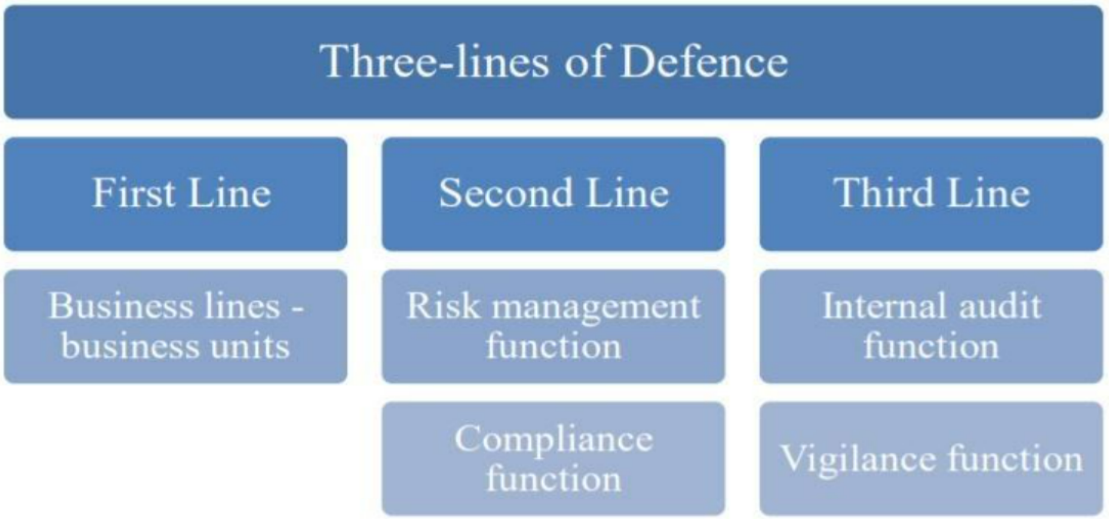

Figure 1: RBIA - The Third Line of Defence

The RBIA Circular goes on to state that the "Risk Management Function" of the NBFC should focus on identification, measurement, monitoring, and management of risks, development of risk policies and procedures, use of risk management models, etc. While RBIA should undertake an independent risk assessment for the purpose of formulating a risk-based audit plan which considers the inherent business risks emanating from an activity/ location and the effectiveness of the control systems for monitoring such inherent risks. Such an internal audit framework may also help in anticipating areas of potential risks and mitigating such risks.

Implementing the RBIA Framework

The RBIA Circular, however, does not provide a technical guide on how to implement such an internal audit framework and we have to turn to the guidance provided by the ICAI and the ICMAI, the accounting and auditing standard setting bodies for guidance.

RBIA Objectives

As per the RBIA Circular -

> *An effective Risk-Based Internal Audit (RBIA) is an audit methodology that links an organisation'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 organisation's internal controls, risk management and governance related systems and processes.*

Based on an analytical reading of the above statement, we can frame the following questions for the internal auditor to answer as part of conducting the RBIA-

- Whether risk management process (RMP) are operating as intended?
- Whether RMPs are of sound design?
- Whether the response to risk by management are adequate and effective to reduce such risk to level acceptable by the Board/ Senior Management?

- Whether sound internal control mechanism is in place to mitigate risks?

Before, however, the auditor can effectively answer these questions that NBFC should have a well defined enterprise-wide risk function in place and outputs of the management's risk assessment exercises form audit inputs for the internal auditor. Guidance provided by the audit standard setting institutes recommend that the auditor assess the organisation's "Risk Maturity" and use it as the basis to decide the audit approach.

Risk Maturity

The ICAI Guide on Risk-based Internal Audit ('Guide') defines the following risk maturity levels -

Risk Maturity	Key Characteristics
"Risk Naive"	No formal approach developed for risk management
"Risk Aware"	Scattered silo based approach to manage risk. No enterprise level processes and controls
"Risk Defined"	Strategy and policy in place. Defined Risk Appetite
"Risk Managed"	Enterprise wide approach to risk management in place. Risk register in place.
"Risk Enabled"	Risk management and internal control fully embed in the business process. Increased readiness to convert market uncertainties to opportunities

Table 2: Risk Maturity Levels

Source: ICAI Guide on Risk-based Internal Audit

Maturity Level to decide Audit Approach/ Strategy

The Guide goes on to provide the following recommendations in terms of deciding the audit approach and objectives -

	Risk Naive	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
Risk Maturity Report	No formal RMP	Poor RMP	RMP Deficiencies	RMP Managed Organisation	RMP Enabled Organisation
Consulting objectives	To promote, guide and facilitate RM	To promote, guide and facilitate RM	To embed RM	To improve RM	Need based improvement
Audit plan based	TAP	TAP	RBIA and supplement with TAP	RBIA	RBIA
Assurance on	Control Processes	Control Processes	RMP and control processes	RMP	RMP
RM = Risk Management *RMP = Risk Management Process* *TAP = Traditional Audit Practice*					

Table 3: Audit Strategy Based on Risk Maturity

(source: ICAI Guide)

Effectively, for NBFCs that have not reached a certain Risk Maturity Level, the Guide recommends that the internal auditor base the internal audit report on traditional audit practices - transactional checks and test of internal controls. And, the auditor should include the observations of the company's risk maturity along with recommendations to attain the "risk managed/ enabled" maturity level. NBFCs that already have a sufficiently mature ERM (described in the following section) in place, the internal auditor can straightaway apply the RBIA approach.

To reiterate, the traditional audit practices will remain relevant for the first 3 stages of risk maturity. The fact that for an NBFC at either of these three levels, it is still the traditional approach and not RBIA approach, is not a deviation from RBIA; in fact, this is precisely what RBI predicates. However, given the size of the NBFC and the significance of risk management at that level, it becomes overwhelmingly important for the NBFC to bring itself up on the risk maturity level. That objective becomes more pressing than the objective of risk-based audit.

Enterprise-wide Risk Management (ERM)

Hence, having an enterprise wide risk management framework becomes a prerequisite for the auditor to be able to adopt a full fledged RBIA approach in the conduct of the internal audit.

Such an ERM framework calls for the following -

- The NBFC should maintain a register of risks that contains the universe of risk sources across the NBFC's lines of business and support function

- The Board/ Senior Management have framed a Risk Appetite Statement that includes the NBFC's risk tolerance levels
- The management has performed assessment of the risks,and periodically performs such assessment by using the following method -

Step1: Assess the NBFC's inherent risk[2] and assigned a risk score (higher the risk level, higher the risk score) ○ For the purposes of assigning the risk score, management should have taken into account the impact or consequences and the likelihood of such risk. **Step 2:** Assess the risk mitigation and internal control processes that are in place and assigned control score ○ For the purposes of assigning the control score, management should have taken into account the control's design and implementation effectiveness **Step3:** Arrive at a residual risk score by using the control scores to adjust the inherent risk score -
Residual Risk = Inherent Risk - Internal Controls

Table 4: Risk Assessment

Note that the method described above is both broad and illustrative. ISO has published the ISO-31010 providing a standard for risk assessment; organisations, however, may use varying methods of arriving at their risk scores.

Audit Coverage

The ICAI Guide recommends that the audit coverage should be based on the risk assurance that the Board/ Senior Management requires and such information may be derived from the risk statement/ risk appetite statement. E.g. The Board/ Senior Management may have a low risk tolerance for risks related to money laundering and corruption and the internal auditor should have such risk included in their audit coverage. The audit coverage forms part of the audit plan along with other aspects such as identification of audit groups (sections of business processes, like product verticals, in which risks are logically bundled), allocation of resources, etc.

The internal auditors may select individual risks or controls to check, where -

- Their residual risk scores are high, especially, where they exceed Board/ Senior Management's risk tolerance levels,
- Their likelihood or impact levels are high,
- Their control score is high, especially, where the corresponding residual risk score is near the tolerance limits - whether internal control measure are overestimated,
- Their residual risk score is near, although below, the risk tolerance levels - whether residual risk is underestimated,
- The external auditor or regulator has made observation regarding such risks or controls.

[2] Inherent risk is the risk inherent to the business without taking into account any risk mitigation or control measures

The auditor, prima facie, accepts the risk scores assigned by management as the basis for selection; however, the auditor would be expected to examine and report cases where there appears to be an error on the face of the risk register and assessed scores.

Report

The performance of the RBIA culminates in preparation of the Internal Audit Report. The RBIA Circular prescribes that the Report should cover -

> *… the objectives, scope, and results of the audit assignment and make appropriate recommendations and / or action plans*
> *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.*

Accordingly the Internal Audit Report should, at least, cover the following aspects -

Content of the Internal Audit Report
• The Assessment of NBFC's Risk Maturity Levels • Opinion whether risk mitigation and internal control processes are being followed • Opinion whether risk mitigation and internal control processes are adequate • Report on whether there are issues with management's assessment of inherent risks • Assessment of control scores and opinion on residual risk vis-e-vis risk tolerance level

Table 5: Internal Audit Report

The Senior Management of the NBFC is responsible for taking appropriate action pursuant to the internal audit findings within given timelines and the status on closure of the audit report should be placed before the Board/ Audit Committee of the Board.

Bird's Eye View of the Internal Audit Process

The following flowchart presents a high level view of the internal audit process -

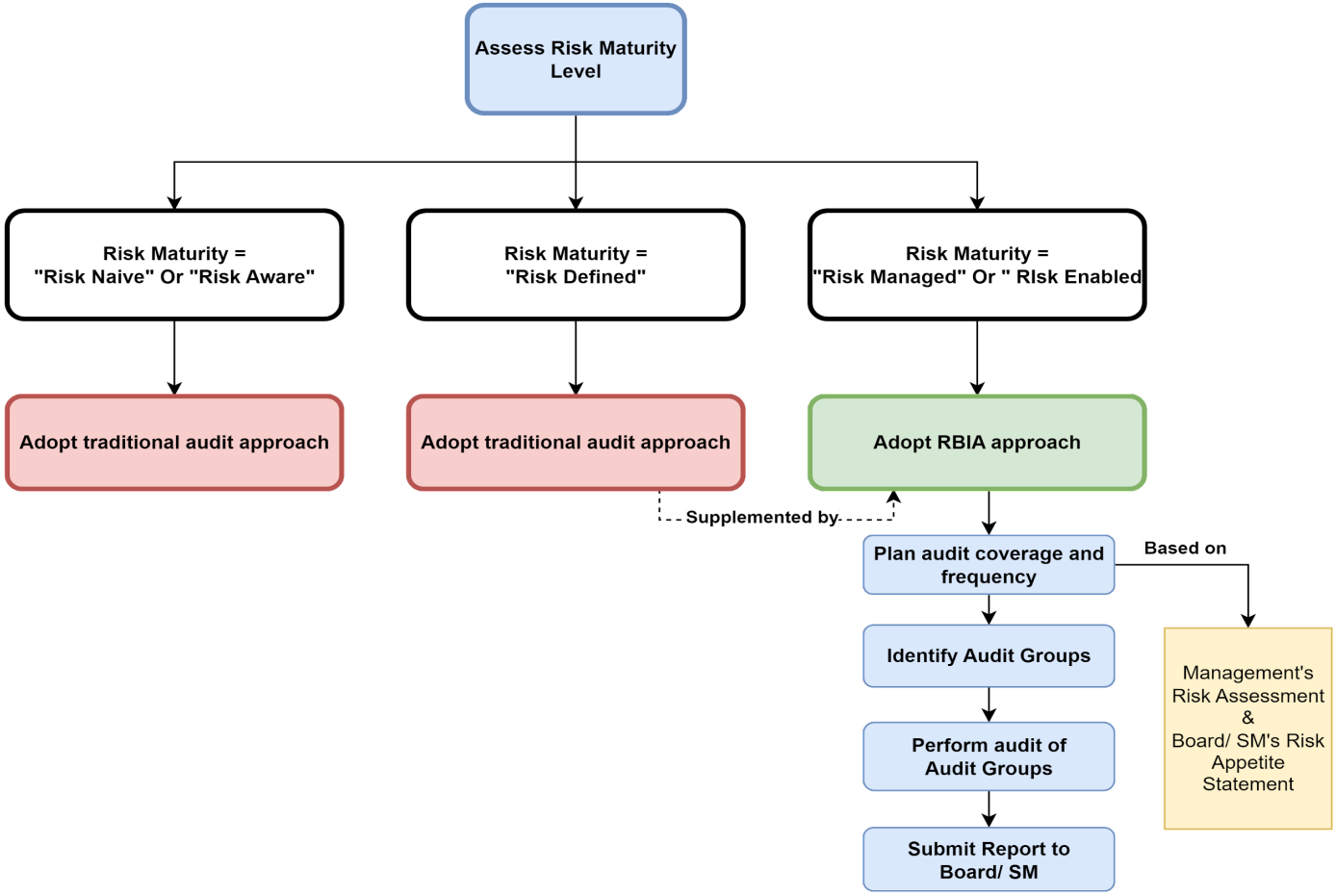

Figure 2: Audit Process

Alternative Framework

Certain literature on RBIA suggests that the internal audit function perform the risk assessment tasks. The RBIA Circular backs such a framework when it states-

> *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 Circular, however, also specifies-

> *While the Risk Management Function should focus on identification, measurement, monitoring, and management of risks, development of risk policies and procedures, use of risk management models, etc., RBIA should undertake an independent risk assessment for the purpose of formulating a risk-based audit plan which considers the inherent business risks emanating from an activity / location and the effectiveness of the control systems for monitoring such inherent risks.*

For substantially large NBFCs for which RBIA is prescribed, it might be too much of an ask for the internal auditor to perform an adequate risk assessment of the entire organisation right down to the nitty gritty. And it becomes especially challenging if the NBFC does not have an adequate enterprise-wide MIS and risk management process in place.

Conclusion

With the RBI recognising the systemic importance of NBFCs large in size, the RBIA mandate has been placed upon them. The objective being such NBFCs put in place an adequate risk management framework (RMF) and the internal audit function provide an independent assurance that such RMF is working as desired. There is debate as to whether risk assessment in the form of maintaining a comprehensive risk register, assessing residual risk levels, etc., should be performed by senior management as part of the risk function or whether it should be undertaken by the internal auditor who may be an external party. The principle that - management knows the business best - tends to support the approach in which the NBFCs management perform the risk assessment and the internal auditor uses such assessment to formulate the audit plan and apply the tools in his audit toolbox to examine the risk management processes (*"RBIA is an audit of the risk management processes and not an audit of risk"*). Notwithstanding which approach is selected by the NBFC's Board/ Senior Management, it is evident that it will be nigh impossible for the internal auditor to deliver as per the RBIA Circular without a well defined and implemented enterprise-wide risk management and MIS in place. Hence, the RBIA assurance framework effectively also imposes on the specified NBFCs the need to strengthen their risk function and have an adequate ERM implementation in place.