Aditya Birla Housing Finance Limited

Policy on Risk Based Internal Audit

Version: ABHFL RBIA Policy/2.0

Contents

Name & Designation	Date
Approved By	
Board of Directors	**27 Apr 2023**
Audit Committee of Board	**27 Apr 2023**
Proposed By	
Internal Audit	**27 Apr 2023**

Document Owner, Version Control & Review Process

Particulars	Details
Version Control	This version dated April 27, 2023, is the Risk-Based Internal Audit Policy of Aditya Birla Housing Finance Ltd. The Policy may be reviewed/modified if warranted by changing regulatory requirements.
Version No.	ABHFL/RBIA Policy/2.0
Document owner(s)	Internal Audit, Aditya Birla Housing Finance Ltd.
Next Review Date	April 2024.
Process for any modification/revision	Approval from the following will be required for any modifications/revisions in this document: Audit Committee of the Board (ACB) / Board of Directors (Board)
Summary of Key Changes	Risk Assessment Methodology added in the Policy. Information Systems Audit Framework added in the Policy.

1. Omnibus clause

All extant & future guidelines issued by the Reserve Bank of India, National Housing Bank, and/or SEBI and any Statutory laws from time to time would be the directing force for this Policy and will supersede the contents of this Policy. This derives from the following Circular, as well as draws directly from the relevant guidelines of the ICAI on these aspects.

Circular Ref. No.	Circular	Issue Date
RBI/2020-21/88 Ref.No.DoS.CO.PPG./SEC.05/11.01.005/202021	Master Direction – Risk Based Internal Audit	Feb 3, 2021
RBI/2021-22/53 DoS.CO. PPG.SEC/03/11.01.005/2021-22	Master Direction – Risk Based Internal Audit (applicable to HFCs)	Jun 11, 2021

2. Objective

In conformance to the NHB Circular, this policy is instituted to define the internal audit activity's purpose, authority, and responsibility.

- The internal audit policy establishes the internal audit activity's position within the organization, including the nature of the Head Internal Audit's functional reporting relationship with the ACB / Board; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit policy resides with the ACB / Board.
- ABHFL has, over the years, instituted a risk-based approach in an internal audit that also leverages the comprehensive documentation of inherent risks and controls in the management processes across all lines of businesses and support functions. Thematic areas intrinsic to the core businesses of the company and their corresponding control and support functions are covered in the audit planning. This new stipulation from NHB necessitates a significant upgrade of the approach already followed in ABHFL, by way of establishing a formal documented framework of RBIA, covering key aspects of methodology such as assessing inherent and residual risk, quantifying risk and controls with scores, ascertaining functional level risks and providing consolidated views of entity-level risks to Audit Committee of the Board. Details are outlined below.

3. Definitions

a. Internal audit

Internal auditing is an independent, objective assurance 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.

b. Risk-based internal audit

Risk-based internal audit involves the assessment of the risks' maturity level, expressing an opinion on the adequacy of the policies and processes established by management to manage the risks. Risk-based internal audits mainly report on risk management that includes identification, evaluation, control, and monitoring of the risk. A risk-based internal audit mainly focuses on the objectives rather than looking only at the controls and transactions.

Objective of risk-based internal audit is to assure the ACB / Board that:

i. The risk management processes that management has put in place within the organization (covering all risk management processes at the corporate, divisional, business unit level, etc.) are operating as intended.
ii. These risk management processes are of sound design.
iii. The responses that management has made to risks that they wish to treat are both adequate and effective in reducing those risks to a level acceptable to the ACB / Board.
iv. And a sound framework of controls is in place to sufficiently mitigate those risks that management wishes to treat.

4. Mission of internal audit

To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

5. Reporting structure

The Internal Audit function headed by the Head Internal Audit must have organizational independence. Functional reporting of the Internal Audit function to the Audit Committee of the Board would encompass the following areas:

- Approving, reviewing, and updating the internal audit policy.
- Approving the risk-based internal audit plan.
- Approving the internal audit budget and resource plan.
- Receiving communications from the Head IA on the internal audit activity's performance relative to its plan and other matters.
- Approving decisions regarding the appointment and removal of the Head Internal Audit and approving the remuneration of the Head Internal Audit. Wherever applicable, the specialist service provider arrangement shall also be subject to approval by the ACB.

- Making appropriate inquiries of management and the Head IA to determine whether there are inappropriate scope or resource limitations.

6. Responsibilities

a) Board of Directors/ Audit Committee of Board (ACB):

- The Board of Directors (the Board) and Audit Committee of Board (ACB) are primarily responsible for overseeing the internal audit function in the organization.
- The internal audit function shall be carried out effectively to ensure that it adds value to the organization. For the purpose, the ACB / Board shall approve a 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.
- The ACB / Board is expected to review the performance of RBIA. The ACB/Board should formulate and maintain a quality assurance and improvement program that covers all aspects of the internal audit function.
- The Board shall examine the feasibility of prescribing at least one stint of service in the internal audit function for those staff possessing specialized knowledge useful for the audit function, but who are posted in other areas. Further, it may prescribe for minimum period of service for internal audit staff, if required.

b) Senior Management:

- The senior management is responsible for ensuring adherence to the internal audit policy guidelines as approved by the ACB / Board and development of an effective internal control function that identifies, measures, monitors and reports all risks faced. It shall ensure that appropriate action is taken on the internal audit findings within given timelines and status on closure of audit reports is placed before the ACB / Board.
- The senior management is responsible for establishing a comprehensive and independent internal audit function which should promote accountability and transparency. It shall ensure that the RBIA Function is adequately staffed with skilled personnel of right aptitude and attitude who are periodically trained to update their knowledge, skill and competencies.
- A consolidated position of major risks faced by the organization shall be presented at least annually to the ACB / Board, based on inputs from all forms of audit.

- Internal Audit activity must be free from interference in determining the scope of internal auditing, performing fieldwork, and communicating results. The Head IA must disclose any such interference to the Audit Committee and discuss the implications.

- The Head Internal Audit shall report to the ACB and Chief Audit Officer of Aditya Birla Capital Ltd by way of functional reporting, have a direct interface with the ACB Chairman. ACB shall meet the Head Internal Audit at least once in a quarter, without the presence of the senior management (including the MD & CEO/WTD).

- For administrative purposes the Head Internal Audit shall report to the MD & CEO, however, shall retain functional independence from management. For matters of performance appraisal of the Head IA, wherein the "Reporting Authority" is the MD & CEO, the ACB shall be the "Reviewing Authority" and the Board the "Accepting Authority".

- Internal Audit shall update the status of completion of the audits (corresponding to the approved audit calendar) along with the key findings of the audits, in the quarterly Audit Committee.

- The Head Internal Audit shall not have any reporting relationship with the business verticals or support/control functions and shall not be given any business targets. Further, the Head Internal Audit appointed will be appointed for a reasonably long period, preferably for a minimum of three years.

- Remuneration policies for the internal audit function and the Head Internal Audit should be structured in a way to avoid creating a conflict of interest and compromising the audit's independence and objectivity.

7. Three lines of defence and functional boundaries

- Internal Audit is the third line of defence and is an independent assurance unit, without any role, governing or operating, that may overlap with the operating management responsibilities, or the first line of defence, or the second line of defence. Reports/feedback/inputs from the first and second lines of defence may be sought and used by the internal audit function as a prudent measure of assessing the management awareness and mitigation of risks inherent in the business processes.

- The Head Internal Audit shall not undertake any roles and responsibilities that fall outside of the internal auditing, and safeguards must be in place to limit impairments to independence or objectivity. The internal audit function shall not perform other activities ordinarily falling under the ambit of operating management, including functions like compliance or risk management activities.

- Thus, internal audit may use inputs from the Operational Risk Management unit and/or the ORMC, the Compliance Unit, the Fraud Control Unit, the CISO function, as well as consider inputs from other management reviews/audits that any operating functions may have in place.

- When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by managing risks.

8. Planning the risk-based internal audit scope

- To develop the risk-based plan, the Head Internal Audit 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. The Head IA must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

- Risk assessment methodology including Audit frequency has been defined in the relevant section in this document.

- Further, to ensure that risk assessment is comprehensive, forward-looking, and dynamic, IA shall work in close coordination with various stakeholders (including key Control functions like ORM, Information Security Risk Management, Compliance, etc.) to seek their inputs on various qualitative and quantitative parameters (both internal and external to ABHFL) as part of ongoing engagement in RBIA approach.

- Internal Audit shall independently review the documentation of the risk assessment/identification, considering the inherent risks emanating from various business processes, the controls thereof, using Risk Control Matrices ("RCMs") which are created and maintained by the management. Internal Audit shall share the review inputs with operating management wherever modifications are required to improve upon the RCMs' adequacy of coverage.

- Basis above, each auditable unit/ RCM for respective function shall be residual risk rated as Significant/ Very High/ High/ Medium/Low and qualitative assessment-based risk rating (i.e. stable, increasing or decreasing depending on past audit experiences, management inputs, incident reporting, etc.) shall be documented along with the rationale of the same. Inherent risks can move direction basis a variety of factors like fundamental changes in products and services, environmental external business factors, regulatory changes, etc.

- For the controls being assessed, the residual risk scores will be assessed basis the efficacy of controls over a one-year rolling period allowing for sufficient information across all businesses/functions/process areas to be used for a risk assessment at any particular point in time.

- 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 the quantitative assessment, the qualitative approach may be adopted for assessing the quality of overall governance and controls in various business activities.

- The risk assessment methodology should include, inter alia, parameters such as (a) Previous internal audit reports, inspection 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.

- The internal audit function should be kept informed of all developments such as the introduction of new products, changes in reporting lines, changes in accounting practices/policies, etc. Wherever the RBIA based audit plan excludes certain businesses, functions, processes, systems, or parts thereof given the level of inherent risk at the time of annual scoping and plans approvals, these exclusions should be reviewed annually for inclusion in next year's plan. No area should be left unaudited (irrespective of being low risk), for over three years from the date of first exclusion.

- With changing business scenarios within the audit calendar, if any such excluded area needs to be included within the audit, Internal Audit shall recommend the inclusion to senior management and the Audit Committee of the Board in the immediate next quarterly ACB meeting, seek the approval and commence upon the audit of areas as per decided timeline.

- The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

- The audit scope and calendar shall be presented to the ACB for approval.

- The internal audit function must identify and consider the expectations of senior management, ACB / Board, and other stakeholders for internal audit opinions and other conclusions.

- The Audit Committee's advice on the risk acceptance levels in certain areas/processes will need to be factored in the risk-based audit approach being implemented as the level of assurance sought in these areas may differ amongst different areas/processes depending on the impact on the organization and ACB / Board.

- The Head Internal Audit and the Internal Audit functionaries should have the authority to communicate with any staff member and get access to all records that are necessary to carry out the entrusted responsibilities.

9. Risk Assessment Methodology

1. Corporate Functions:

Inherent risk assessment

Based on the assessment of the likelihood and impact of each risk, an inherent risk score will be assigned. The inherent risk score will be calculated by multiplying the "likelihood" and "impact" ratings of each risk.

Control framework assessment

Control assessment will be performed basis level of Controls Automation, Maturity of risk control self-assessment framework, Documentation of Controls and past Audit observations.

Residual risk assessment

Based on an evaluation of the control environment and the inherent risk for each function, the residual risk would be arrived at basis the below grid and audit frequency will be decided accordingly.

Control Risk	Inherent risk				
	Low	**Medium**	**High**	**Very High**	**Significant**
Robust	Low Risk	Low Risk	Low Risk	Medium Risk	Medium Risk
Effective	Low Risk	Low Risk	Medium Risk	Medium Risk	Medium Risk
Satisfactory	Low Risk	Medium Risk	Medium Risk	High Risk	High Risk
Improvement needed	Medium Risk	Medium Risk	High Risk	Very High Risk	Significant Risk
Significant Improvement needed	Medium Risk	High Risk	Very High Risk	Significant Risk	Significant Risk

Residual Risk	Audit Frequency
Low Risk	30 - 36 months
Medium Risk	18 - 24 months
High Risk	12 - 15 months
Very High Risk	9 - 12 months
Significant Risk	6 - 9 months

2. Branches

Risk Assessment for Branch Audit

Following risk assessment parameters will be considered for assessing the risk pertaining to each branch. Weighted score will be assigned to each branch, basis which risk level is assigned, and audit frequency is arrived for individual branch. All the branches will be audited once in 3 years.

Risk Level	Audit Frequency
Low Risk	30 - 36 months
Medium Risk	18 - 24 months
High Risk	12 - 15 months
Very High Risk	9 - 12 months
Significant Risk	6 - 9 months

3. IT Applications

Risk Assessment for IT Applications

IT Applications will be tagged as Critical or Non-critical. Below would be parameters and Audit frequency for the IT Applications.

- Internet based / Intranet based
- Hosted on Cloud / Third Party sites / On Premise
- Applications Used for business processes / support processes.

Criticality	Audit Frequency
Critical	12-18 months
Non-Critical	24-36 months

10. Audit activity and outcome

The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

- When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization, and the expectations of senior management, ACB / Board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.

- Final communication of engagement results must include applicable conclusions, as well as applicable recommendations and/or action plans.

- It should cover the objectives, scope, and results of the audit assignment and make appropriate recommendations and/or action plans. Any delays in execution of audits, scope limitations, or dissonance in perspective of internal audit and management in risk perception of an audit observation must be brought to the notice of the ACB as part of the routine audit reporting process.

- Reporting to the ACB by way of a suitable template shall be established to showcase the residual risk levels. Any residual risks above an acceptable threshold are required to be accompanied by management action plans to remedy the open risks. These updates may also consider the larger context of business risks (internal and external factors), also factoring in controllable and uncontrollable risks.

- The IT reports (Information Technology General Controls reports) shall be communicated to the IT Committee of the Board as well, in addition to the ACB. The IT audit shall be conducted by a Certified Information System Auditor. If the Internal Audit function feels the need to include certain observations arising out of system dependency/functionality issues in other areas of internal audit the same may be reported to the IT Committee of the Board at the discretion of the Head IA.

- Internal Audit shall progressively automate areas of the audit through effective use of data, to an extent possible through checks which can be run on system data extracts and incorporate the results of such reviews into the regular audit communication/reporting to management, senior management, and the ACB. The processes/areas/controls which require manual testing shall continue to be on traditional methods of audits, whereas the overall area under audit could include a combination of both data analytical automated checks as well as manual checks, to

give a cogent review based on an objective understanding of the adequacy of design and operating effectiveness of the business processes.

- Such internal, data-based automated checks shall constitute the 'internal' part of the In-house / Specialist Service Provider model of auditing that the company has adopted, while the overall responsibility of the Internal Audit functioning rests with the management, represented by the Head Internal Audit.

  The Head IA must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action. Further, 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. Staffing

- **Proficiency**

  Internal auditors must possess the knowledge, skills, and other competencies needed to perform their responsibilities. The internal audit function collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

- **Use of external staffing expertise**

  Company shall use the services of an external professional firm for rendering specialist services for the internal auditing activity, under the supervision and responsibility of the in-house Internal Audit function, headed by the Head IA. Such arrangements would need the explicit approval of the ACB. The professional independence of the internal audit function shall extend by default to all such external arrangements.

  Any audit areas that may require external expertise shall be considered for external resourcing subject to guidance and approval of the ACB.

  In the journey towards building in-house capability, when using a hybrid In-house / Specialist Service Provider resourcing model, the final consolidation of audit reports/findings will suitably synchronize the outputs of the external team/s with the internal team in one set of reports, factoring the nuances of cross dependency of functional/business areas/processes being audited, and best optimization of resources. The arrangement shall retain the flexibility to demarcate specific areas for external resourced auditing as well, depending on areas/themes under consideration.

Ownership of internal audit reports shall continue to rest with the internal audit function of the company.

Internal audit function shall be guided by the **Code of Ethics** – Principles outlined by the Institute of Internal Audit, upholding the following principles:

- **Integrity** - The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.
- **Objectivity** - Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal

auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their interests or by others in forming judgments.

- **Confidentiality** - Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.
- **Competency** - Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

12. Information Systems (IS) Audit

The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications etc.

IS Audit should form an integral part of Internal Audit system of the organisation.

Coverage

IS Audit should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up.

IS Audit should also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organization.

During the process of IS Audit, due importance shall be given to compliance of all the applicable legal, statutory and regulatory requirements.

Personnel

IS Audit may be conducted inhouse by the internal audit team. In case of inadequate internal skills, the internal audit team may evaluate appointment of an outside agency having enough expertise in area of IT/IS audit for the purpose.

There should be a right mix of skills and understanding of legal and regulatory requirements to assess the efficacy of the framework vis-à-vis these standards.

IS Auditors should act independently of the Management both in attitude and appearance.

In case of engagement of external professional service providers, independence and accountability issues may be properly addressed.

Periodicity

The periodicity of IS audit shall be based on the size and operations of the organisation but may be conducted at least once in a year.

IS Audit shall be undertaken preferably prior to the statutory audit so that IS audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.

Compliance

The management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. The framework may provide for an audit-mode access for auditors.

Usage of Computer-Assisted Audit Techniques (CAATs):

The organisation shall adopt a proper mix of manual techniques and CAATs for conducting IS Audit. CAATs may be used in critical areas where a large volume of transactions is reported particularly for critical functions or processes having financial/regulatory/legal implications.

13. Quality assurance program for internal audit

- The Internal Audit function shall put in place a framework for the Audit Committee of the Board to assess the adequacy of the internal audit activity, on an annual basis. The function may consult the ACB, or act upon the ACB's guidance on any of the inputs received during the year as well.
- A proposed set of parameters for the annual assessment is given in Annexure 1 (the annexure can be changed to align with changing dynamics of the requirement of the ACB and/or the management, with the approval of the ACB on the Head IA's recommendation in future without recourse to amending the entire policy).

14. Review and modification

Any modification in the policy on ongoing basis evolution of the RBIA and any other business dynamics can be done with the approval of the Head IA and ACB / Board. The timeline for the annual review of the policy to be done by Head IA will be considered as one year from the date of the approval of the latest extant version of the policy by the ACB / Board.

15. Annexure – 1

Parameters for Performance Appraisal of the Internal Audit Function by Audit Committee

Suggested values:
1-Excellent, 2-Very Good, 3-Satisfactory, 4-Needs improvement, 5-Unsatisfactory

Parameters	Rating	Qualitative comments if any
Appropriate risk-based scoping factoring the complexities and nature of businesses		
Adherence to approved Audit Calendar		
The clarity in stating observations (Criteria, Condition, Consequence, Corrective action)		
Driving remediation with follow-through with management on open issues		
Understanding of business processes		

Annexure – 2

Risk Assessment Methodology

1. Corporate Functions

Inherent risk assessment

Based on the assessment of the likelihood and impact of each risk, an inherent risk score has been assigned. The inherent risk scores have been calculated by multiplying the "likelihood" and "impact" ratings of each risk. Below mentioned rating methodology has been used rating the likelihood and impact of each risk.

Step 1 – Impact assessment

Rating	Descriptor	Definition						
		Financial Risk	Reputational Risk	Compliance Risk	Credit Risk	ALM Risk	Technological Risk	Operational Risk
5	Extreme	Potential Financial loss / Reporting error which is estimated to Approx INR 1 Crore or more*	The impact could lead to significant damage to the reputation / brand / market value and negative publicity causing customer impact	Significant Compliance breaches leading to prosecution and fines, litigation and / or including class actions, incarceration of leadership	Significant impact due to potential breach of credit assessment and underwriting parameters leading to estimated impact on customer base having increased counterparty risk	Significant failure of potential ALM framework having huge non-manageable liquidity mismatches/ blockage of funds	Significant impact on the data protection / information security controls and loss of tangible/ intangible technological assets / infrastructure - Wide-rage data confidential integrity and availability breach	Significant risk having very high impact on the operational efficiency of the process and in-turn on the business continuity or fallback arrangements of the function / entity
4	Major	Potential Financial loss / Reporting error which is estimated to Approx INR 75 lakhs to INR 1 crore*	The impact could lead to sizable damage to the reputation / brand / market value and negative publicity causing customer impact	Compliance breach having minimum or no options for mitigation under the respective regulatory requirement	High impact due to potential breach of credit assessment and underwriting parameters leading to estimated impact on customer base having increased counterparty risk	Failure of potential ALM framework having limited non-manageable liquidity mismatches/ blockage of funds	- High/ Medium impact on the data protection / information security controls and loss of tangible technological assets / infrastructure - Limited data security breach leaking confidential information	- Risk having high impact on the operational efficiency of the process and in-turn on the business continuity or fallback arrangements of the function / entity - Loss of assets / temporary non-

Rating	Descriptor	Definition						
		Financial Risk	Reputational Risk	Compliance Risk	Credit Risk	ALM Risk	Technological Risk	Operational Risk
								availability of the asset
3	Moderate	Potential Financial loss / Reporting error which is estimated to Approx INR 50 Lacs to INR 75 Lacs*	The impact could lead to slight damage to the reputation / brand / market value and negative publicity causing customer impact	Compliance breach having options for mitigation under the respective regulatory requirement	Moderate impact due to potential breach of credit assessment and underwriting parameters leading to estimated impact on customer base having increased counterparty risk	NA	- Medium impact on the data protection / information security controls and loss of tangible technological assets / infrastructure - No data security breach leaking confidential information	- Risk having limited impact on the operational efficiency of the process and in-turn on the business continuity or fallback arrangements of the function / entity - Incorrect usage of the asset leading to operational inefficiency
2	Minor	Potential Financial loss / Reporting error which is	The impact could lead to inconsequential or very limited damage to the reputation / brand /	Compliance breach which may not be reportable incident or does not significantly requires	Minor impact due to potential breach of credit assessment and underwriting	NA	- Minor impact on the data protection / information security controls and no loss of	- Risk having low impact on the operational efficiency of the process

Rating	Descriptor	Definition						
		Financial Risk	Reputational Risk	Compliance Risk	Credit Risk	ALM Risk	Technological Risk	Operational Risk
		estimated to Approx INR 20 Lacs to INR 50 Lacs*	market value	follow up / mitigation	parameters leading to estimated impact on customer base having increased counterparty risk		tangible technological assets / infrastructure - No data security breach leaking confidential information	and in-turn no or limited impact on the business continuity of the function / entity - Minor / incidental delay in attending to the gaps in asset safeguarding / management
1	Incidental	Potential Financial loss / Reporting error which is estimated to Approx INR 20 Lacs or less*	Incidental or no reputational risk	Not reportable or inconsequential compliance breach to the regulatory / compliance requirement	Incidental impact due to potential breach of credit assessment and underwriting parameters leading to estimated impact on customer base having increased counterparty risk	NA	- Incidental impact on the data protection / information security controls and no loss of tangible technological assets / infrastructure - No data security breach leaking confidential information	- Incidental / Exceptional impact on the operational efficiency of the function / entity

Step 2 – Likelihood assessment

Rating	Annual Frequency	
	Descriptor	Definition
5	Frequent	Such an event has occurred or can occur in estimated next 6 months approximately.
4	Likely	Such an event has occurred or can occur in estimated next 12 months approximately.
3	Possible	Such an event could occur in the foreseeable future (maybe 1 to 5 years) even though it has not occurred yet.
2	Unlikely	Such an event is unlikely to occur in the foreseeable future (maybe 1 to 5 years)
1	Rare	Such an event will rarely occur in the foreseeable future (maybe 1 to 5 years)

Step 3 – Inherent risk scoring

Inherent Risk Score = Impact Score * Likelihood Score

Inherent risk scoring and classification			IMPACT				
			Incidental	**Minor**	**Moderate**	**Major**	**Extreme**
			1	2	3	4	5
LIKELIHOOD	**Rare**	**1**	1	2	3	4	5
	Unlikely	**2**	2	4	6	8	10
	Possible	**3**	3	6	9	12	15
	Likely	**4**	4	8	12	16	20
	Frequent	**5**	5	10	15	20	25

Risk scores	Category
1-2	Low Risk
3-6	Medium Risk
7-11	High Risk
12-18	Very High Risk
19-25	Significant Risk

Control framework assessment

Based on an evaluation of the control environment, the control framework assessment has been conducted across eight parameters as identified below.

Step 1 – Risk classification based on defined parameters

Parameters	Control framework classification based on the responses received				
	Robust	Effective	Satisfactory	Improvement needed	Significant Improvement needed
Number of internal issues identified with high-risk rating	-	0	1-2	>2-5	>5
Number of internal issues identified with medium-risk rating	0	0 -2	>2-5	>5-10	>10
Number of internal issues identified with low-risk rating	0	0 -2	>2-5	>5-10	>10
Number of regulatory non-compliances identified (internal and external)	0	0	0-1	>1-5	>5
1. Whether risk and control self-assessment has been done for the area? 2. If yes, provide the number of issues identified.	0	0 -2	>2-5	>5-10	>10
Assessment for level of automation	>80%	>65-80%	>50-65%	>35-50%	0-35%
Assessment for documentation of controls for risk identified	>90%	>60-90%	>40-60%	>20-40%	0-20%

Step 2 – Assigning weights to control framework parameters

Control framework	Weights
Robust	1
Effective	2
Satisfactory	3
Improvement needed	4
Significant Improvement needed	5

Step 3 – Assigning control framework rating and scoring

Total Score	Control Framework Rating
>0, but <=1	Robust
>1, but <=2	Effective
>2, but <=4	Satisfactory
>4, but <5	Improvement needed
5	Significant Improvement needed

- If RCSA is not documented - Control classification - Very weak
- If RCSA is documented - Review not performed - Control classification - Very weak
- If RCSA is documented - Review performed - Control classification - Go by Matrix
- If Automation is not feasible / not available - Control classification - Very Weak
- Last two years IA reports are considered for IA issue identification

Residual risk assessment

Based on an evaluation of the control environment and the inherent risk for each function, the residual risk assessment has been derived to arrive at the audit frequency

Control Risk	Inherent risk				
	Low	**Medium**	**High**	**Very High**	**Significant**
Robust	Low Risk	Low Risk	Low Risk	Medium Risk	Medium Risk
Effective	Low Risk	Low Risk	Medium Risk	Medium Risk	Medium Risk
Satisfactory	Low Risk	Medium Risk	Medium Risk	High Risk	High Risk
Improvement needed	Medium Risk	Medium Risk	High Risk	Very High Risk	Significant Risk
Significant Improvement needed	Medium Risk	High Risk	Very High Risk	Significant Risk	Significant Risk

Residual Risk	Audit Frequency
Low Risk	30 - 36 months
Medium Risk	18 - 24 months
High Risk	12 - 15 months
Very High Risk	9 - 12 months
Significant Risk	6 - 9 months

2. Branches

Risk Assessment for Branch Internal Audit

Following risk assessment parameters are considered for assessing the risk pertaining to each branch. Weighted score is assigned to each branch between 1 to 3, basis which risk level is assigned, and audit frequency is arrived for individual branch. All the branches will be audited once in 3 years.

#	Parameters	Weights	Scoring		
			1	2	3
1	Asset Under Management	20%	Below 2.5% of Total AUM	=> 2.5% <5% of Total AUM	> 5% of Total AUM
2	Non-Performing Assets	25%	<5% of Country Average	=> 5% <= 10% Country Average	> 10% of Country Average
3	Over-Dues	15%	<5% of Country Average	=> 5% <= 10% Country Average	> 10% of Country Average
4	No of Audit Observations	10%	No Observation	1-2	>2 / Not audited
5	No. of Frauds Reported	10%	No Fraud	NA	1 or more
6	No. of Customer Complaints	10%	<=25	>25<=50	>50
7	Net Promoter Scores	10%	>65	30-65	<30

Weighted Score	Risk Level	Audit Frequency
upto 1.25	Low Risk	30 - 36 months
>1.25 to 1.5	Medium Risk	18 - 24 months
>1.5 to 2	High Risk	12 - 15 months
>2 to 2.5	Very High Risk	9 - 12 months
>2.5 to 3	Significant Risk	6 - 9 months

3. IT Applications

Risk Assessment for IT Applications

IT Applications will be tagged as Critical or Non-critical. Below would be parameters and Audit frequency for the IT Applications.

- Internet based / Intranet based
- Hosted on Cloud / Third Party sites / On Premise
- Applications Used for business processes / support processes

Criticality	Audit Frequency
Critical	12-18 months
Non-Critical	24-36 months

****