INTERNAL AUDIT POLICY

(For Base Layer NBFC – Investment and Credit Company)

1. Objective

The objective of this Internal Audit Policy is to establish a comprehensive, independent, and risk-based internal audit framework to:

- Evaluate the adequacy and effectiveness of internal controls *and risk management systems*.
- Assess *the robustness of* risk management systems *against evolving business dynamics*.
- Ensure compliance with applicable regulatory guidelines issued by *the* RBI*, the Ministry of Corporate Affairs (MCA), and other statutory bodies*.
- Safeguard company assets and stakeholder interests.
- Strengthen corporate governance standards.
- Detect and prevent fraud, operational lapses, and financial irregularities.

This policy is aligned with the regulatory prescriptions applicable to NBFC-ICC classified under the Base Layer as per RBI's Scale Based Regulation (SBR) framework *and the statutory mandate under Section 138 of the Companies Act, 2013*.

2. Applicability & scope

This policy applies to:

- All business units and branches
- All operational and functional departments
- All products including lending activities *and digital lending platforms*
- Outsourced activities and third-party service providers *(including Lending Service Providers)*
- Information Technology systems and infrastructure

The Internal Audit shall cover, but not be limited to:

1. Credit operations and loan lifecycle management
2. Asset classification and provisioning *(IRACP norms)*
3. Treasury and liquidity management
4. ALM compliance
5. KYC/AML compliance
6. IT systems*, Information Systems (IS) Audit,* and cybersecurity
7. HR and payroll controls
8. Financial reporting and accounting systems *(including Ind AS/Accounting Standards compliance)*
9. Outsourcing risk management
10. Regulatory reporting and returns *(e.g., XBRL filings)*
    11. Compliance with the Digital Personal Data Protection (DPDP) Act, 2023.

3. Regulatory framework

This Policy is framed in compliance with:

- RBI Master Direction – NBFC – ICC (Non-Deposit Taking)
- RBI Scale Based Regulation (SBR) Framework
- RBI Guidelines on Risk Management Systems
- RBI KYC Master Direction
- IRACP norms applicable to NBFCs
- *Section 138 and Section 177 of the Companies Act, 2013, read with Rule 13 of the Companies (Accounts) Rules, 2014*

- *RBI Guidelines on Risk-Based Internal Audit (RBIA) (adopted as a best corporate governance practice for Base Layer NBFCs)*
- *Applicable Secretarial Standards issued by the ICSI*
- In case of any regulatory amendment, the RBI *and statutory* guidelines shall prevail automatically.

4. Governance structure

4.1 Board Oversight
The Board of Directors shall:

- Approve the Internal Audit Policy *and review it annually*.
- Ensure *the absolute* independence of the Internal Audit function.
- Review significant audit findings.
- Monitor compliance with regulatory directions.
- Ensure corrective actions are implemented in a timely manner.

For NBFC-Base Layer, though *the* constitution of *an* Audit Committee may not be mandatory *under RBI SBR unless the Company crosses the thresholds specified under Section 177 of the Companies Act, 2013 (e.g., paid-up capital of ₹10 crore or more, turnover of ₹100 crore or more, or outstanding loans/borrowings exceeding ₹50 crore)*, the Board shall ensure adequate oversight of audit functions.
4.2 *Audit Committee* (if constituted)
If constituted under Section 177 of the Companies Act, 2013, the Committee shall have a minimum of three directors with independent directors forming a majority.
The Committee may comprise:

- Chief Financial Officer *(as an invitee)*
- Compliance Officer *(as an invitee)*
- Head of Internal Audit *(as an invitee)*
- Independent Director(s), if any *(acting as Chairperson)*
  Responsibilities:
- Approve *the annual* risk-based audit plan.
- Review quarterly audit reports *and the effectiveness of the internal financial controls*.
- Monitor high-risk observations.
- Track unresolved issues.
- Recommend systemic improvements *to the Board*.

Meeting Frequency: Minimum quarterly.

5. Independence of internal audit

- The Internal Audit function shall operate independently of *all* operational management.
- Internal Auditors shall have unrestricted access to *all* records, employees, *properties,* and systems.
- Reporting line shall be directly to the Board or *the* Audit Committee.
- Internal auditors shall not audit activities for which they have *or had recent* operational responsibility.
- Independence shall be documented and reviewed annually *by the Board/Audit Committee*.

6. Appointment of internal auditors

Internal Audit may be conducted by:

- Qualified internal audit team; or
- External Chartered Accountant firm with NBFC expertise.

As per Section 138 of the Companies Act, 2013, the internal auditor shall either be a Chartered Accountant or a Cost Accountant, or such other professional as may be decided by the Board to conduct the internal audit of the functions and activities of the Company.
Selection Criteria:

- Experience in NBFC audit
- Knowledge of RBI regulations *and SBR framework*
- Understanding of risk-based auditing
- Familiarity with IT system audits

Appointment *and remuneration* shall be approved by the Board *(or recommended by the Audit Committee, where applicable).*

7. Risk-based internal audit framework

The Company shall adopt a Risk-Based Internal Audit (RBIA) approach *to prioritize audit resources toward areas of highest risk.*

7.1 Risk Identification Areas

1. **Credit Risk**
   - o Loan sanction process *and due diligence*
   - o Documentation completeness
   - o Asset classification accuracy
   - o NPA recognition
   - o Provisioning adequacy
   - o Recovery process
2. **Liquidity & ALM Risk**
   - o Maturity mismatch
   - o Liquidity gap statements
   - o Stress scenarios
   - o Compliance with ALM policy
3. **Operational Risk**
   - o Process inefficiencies
   - o Fraud detection controls
   - o Delegation of authority compliance
   - *o Cash management and physical security at branches*
4. **Compliance Risk**
   - o KYC/AML adherence
   - o Fair Practices Code compliance
   - o RBI returns filing accuracy
   - o Grievance redressal mechanism
   - *o Corporate/Secretarial compliance under the Companies Act, 2013*
5. **IT & Cyber Risk**
   - o Data security *and privacy (DPDP Act compliance)*
   - o Access controls
   - o System backups
   - o Vulnerability assessments
   - o Digital lending compliance (if applicable)
6. **Outsourcing Risk**
   - o Due diligence of service providers
   - o SLA compliance
   - o Data confidentiality *and localization*

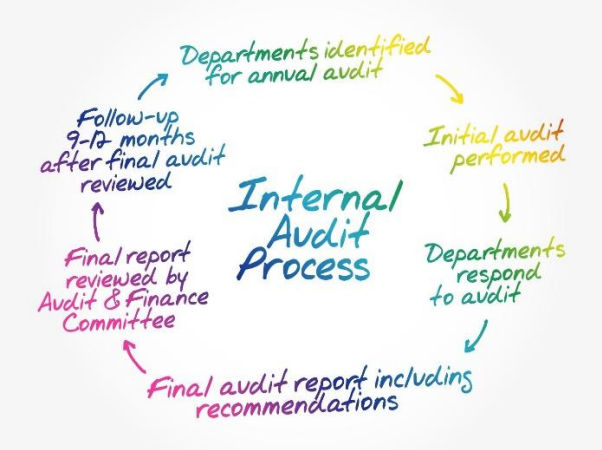
8. Audit Frequency

Risk Category	**Frequency**
Credit & NPA Review	Quarterly
ALM & Liquidity	Quarterly

Risk Category	Frequency
Compliance *& Regulatory Returns*	Quarterly
IT Systems *& Cyber Security*	Annually
HR & Payroll	Annually
Outsourced Activities	Annually or Risk-Based

High-risk branches/segments may be audited more frequently *based on the risk assessment matrix*.

9. Internal audit process



Shutterstock

9.1 Planning Stage

- Annual Risk Assessment
- Preparation of Annual Audit Plan
- Approval by Board/Audit Committee

9.2 Execution Stage

- Sample testing of transactions
- Review of policy compliance
- Control testing
- Staff interviews
- Data analytics *(where applicable, using CAATs - Computer Assisted Audit Techniques)*

9.3 Reporting Stage

The Audit Report shall include:

- Executive summary
- Detailed observations
- Root cause analysis
- Risk grading (High / Medium / Low)
- Regulatory references (if violated)
- Corrective action plan *(CAP)*
- Target completion timeline *and management responses*

10. Risk grading matrix

Each observation shall be classified as:

- **High Risk:** Immediate Board *or Audit Committee* attention required. *Poses significant financial, regulatory, or reputational threat.*
- **Medium Risk:** Corrective action within *a* defined timeline. *Poses moderate operational or compliance risk.*
- **Low Risk:** Process improvement recommendation. *Minor procedural lapses.*

11. Follow-up mechanism

- *An* Action Taken Report (ATR) shall be obtained from concerned departments.
- Follow-up audit shall verify closure *of past observations*.
- Unresolved high-risk items shall be escalated to *the* Board.
- Persistent non-compliance shall be documented and reviewed *for disciplinary action*.

12. Fraud reporting

Internal Audit shall:

- Review fraud risk controls.
- Report suspected fraud immediately to management *and the Audit Committee*.
- Ensure reporting to RBI where required *(via FMR portals)*.
- *Ensure statutory reporting of material frauds (involving amounts of ₹1 crore or above) to the Central Government by the statutory auditors, and reporting of lesser amounts to the Audit Committee/Board, as mandated under Section 143(12) of the Companies Act, 2013 read with Rule 13 of the Companies (Audit and Auditors) Rules, 2014.*
- Recommend strengthening of preventive controls.

13. Regulatory compliance monitoring

Internal Audit shall verify:

- Capital Adequacy Ratio (CRAR) compliance *(minimum 15%)*.
- Net Owned Fund requirements.
- Exposure norms *(as per SBR guidelines for Base Layer)*.
- Fair Practices Code compliance.
- Timely filing of RBI returns *(e.g., DNBS02, DNBS04A, etc., via XBRL)*.
- Compliance with IRACP norms.

14. Documentation & record retention

- Audit working papers shall be securely maintained *to evidence the audit work performed*.
- Records shall be retained for *a* minimum *of* 8 years*, in strict compliance with Section 128 of the Companies Act, 2013*.
- Digital records shall have secure backup *and audit trails.*

15. Policy review

This Policy shall be:

- Reviewed annually; or
- Reviewed upon regulatory changes; or
- Modified based on *changes in the* business risk profile.
- Amendments shall require Board approval.

16. Effective date

This **INTERNAL AUDIT POLICY** has been approved by the Board of Directors of THIRUKOCHI FINCAP LIMITED at its meeting held on 12/03/2026.

Effective Date: 12/03/2026.

Version:1