Document Title: Policy Internal Audit and Guidelines	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Reliance Capital Limited
Policy Internal Audit and Guidelines

Document Title: Policy Internal Audit and Guidelines	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Table of Contents

1. Introduction

- **1.1 Purpose:**
    - The purpose of this policy is to define the framework for the internal audit function, ensuring it provides independent and objective assurance and advisory services to add value and improve the organization's operations.
- **1.2 Applicability:**
    - This policy applies to all departments, functions, and activities within the organization.
- **1.3 Regulatory Framework:**
    - This policy is established in accordance with the Reserve Bank of India (RBI) Master Directions for Non-Banking Financial Company - Core Investment Companies (NBFC-CICs), the Companies Act 2013, and other relevant rules and regulations.
    - It acknowledges the requirements of Section 138 of the Companies Act 2013 concerning internal audit.

2. Objective

- The primary objective of the internal audit function is to evaluate and improve the effectiveness of risk management, internal control, and governance processes.
- Internal audit provides an independent assessment of the adequacy and effectiveness of the organization's system of internal control and the quality of adherence.

3. Scope

- The scope of internal audit includes:
    - Evaluating the design and effectiveness of internal controls.
    - Assessing the reliability and integrity of financial and operational information.
    - Reviewing compliance with laws, regulations, policies, and procedures.
    - Assessing the efficiency and effectiveness of operations.
    - Safeguarding of assets.

4. Internal Audit Governance Framework

- **4.1 Role of the Audit Committee:**
    - The Audit Committee is responsible for overseeing the internal audit function.
    - Key responsibilities include:
        - Approving the annual audit plan.

- Reviewing significant audit findings and management's responses.
- Monitoring the implementation of audit recommendations.
- Ensuring the independence of the internal audit function.

- **4.2 Role of the Internal Audit Function:**
  - The internal audit function is responsible for:
    - Developing and executing the risk-based audit plan.
    - Conducting audits in accordance with professional standards.
    - Reporting audit findings and recommendations to management and the Audit Committee.
    - Following up on the implementation of corrective actions.
- **4.3 Organizational Structure and Independence:**
  - The internal audit function shall have a reporting line to the Audit Committee to ensure independence.
  - The head of internal audit shall have direct access to the Audit Committee.
  - The organizational structure shall ensure that internal auditors are free from any operational responsibilities and conflicts of interest.
- **4.4 Internal Audit Charter:**
  - The Internal Audit Charter defines the purpose, authority, and responsibility of the internal audit function.
  - It establishes the internal audit's position within the organization and its relationship with the Audit Committee and management.

5. Risk-Based Internal Audit

- **5.1 Risk Assessment Methodology:**
  - The internal audit plan shall be based on a documented risk assessment, conducted at least annually.
  - The risk assessment shall consider:
    - Inherent and residual risks.
    - The organization's risk management framework and risk appetite.
    - Input from senior management and the Audit Committee.
    - Qualitative and quantitative factors.
    - The likelihood and impact of risks.

- Risk grades (High, Medium, and Low) shall be assigned to identified risks.

- **5.2 Audit Planning Process:**
  - The annual audit plan shall outline the scope, objectives, timing, and resource allocation for audit engagements.
  - The plan shall be developed by the head of internal audit, considering the risk assessment and audit universe.
  - The plan shall be flexible to accommodate changes in the organization's risk profile.
- **5.3 Audit Universe Definition and Maintenance:**
  - The audit universe shall include all auditable entities, including units, branches, departments, functions, processes, and systems.
  - The audit universe shall be reviewed and updated periodically.
  - Criteria for selecting auditable units shall include:
    - Contribution to organizational goals.
    - Size and impact on the organization.
    - Significance and cost of control.
- **5.4 Audit Frequency and Scheduling:**
  - The frequency of audits shall be determined based on the risk assessment, vulnerability, and significance of the function.
  - The maximum period between audits of any function shall not exceed 36 months.
  - The audit calendar shall be established and communicated to relevant stakeholders.

6. Audit Execution

- **6.1 Audit Methodology and Procedures:**
  - Audits shall be conducted using appropriate methodologies and procedures to achieve the audit objectives.
  - This includes:
    - Planning the audit engagement.
    - Developing audit programs.
    - Gathering and analyzing evidence.
    - Documenting audit work.

- Communicating audit results.

- **6.2 Use of Technology and Data Analytics:**
  - Internal audit shall leverage technology and data analytics tools to enhance audit efficiency and effectiveness.
  - This may include:
    - Audit management software.
    - Data mining and analysis tools.
    - Continuous auditing techniques.
- **6.3 Sampling and Testing Techniques:**
  - Appropriate sampling and testing techniques shall be used to obtain sufficient and reliable audit evidence.
  - Sample sizes shall be determined considering audit objectives, materiality, and the characteristics of the population.
- **6.4 Documentation and Record Keeping Requirements:**
  - Audit work shall be documented in sufficient detail to support audit conclusions and facilitate review.
  - Audit records shall be retained in accordance with the organization's record retention policy and regulatory requirements.

7. Reporting and Communication

- **7.1 Audit Reports: Structure and Content:**
  - A written audit report shall be issued at the conclusion of each audit engagement.
  - The report shall include:
    - Purpose and scope of the audit.
    - Audit findings and recommendations.
    - Management's response and action plan.
    - An overall assessment or opinion.
  - Audit observations shall be classified based on risk (High, Medium, and Low).
- **7.2 Communication with Management:**
  - Audit findings and recommendations shall be communicated to management in a timely and effective manner.

- Discussions shall be held with management to ensure that audit findings are understood and agreed upon.

- **7.3 Reporting to the Audit Committee:**
  - The head of internal audit shall report periodically to the Audit Committee on audit activities, significant findings, and the status of management's corrective actions.
  - Reports to the Audit Committee shall include:
    - Progress against the audit plan.
    - Key risk exposures and control issues.
    - Instances of fraud or suspected fraud.
    - Other matters requiring the Audit Committee's attention.
- **7.4 Escalation Procedures:**
  - Escalation procedures shall be established for unresolved audit issues.
  - The escalation process shall involve increasing levels of management and the Audit Committee, as necessary.

8. Follow-Up and Monitoring of Audit Findings

- **8.1 Management Action Plans:**
  - Management is responsible for developing and implementing action plans to address audit findings.
  - Action plans shall include specific actions, responsible parties, and target completion dates.
- **8.2 Follow-up Process and Responsibilities:**
  - Internal audit is responsible for following up on the implementation of management action plans.
  - The follow-up process shall include:
    - Monitoring the progress of corrective actions.
    - Validating the effective implementation of actions.
    - Reporting on the status of outstanding audit issues.
- **8.3 Monitoring of Implementation:**
  - Internal audit shall maintain a system to track and monitor the status of audit findings and management's corrective actions.

9. Quality Assurance and Improvement Program

- **9.1 Internal Quality Assessments:**
    - Internal quality assessments shall be conducted periodically to evaluate the effectiveness and efficiency of the internal audit function.
    - These assessments shall include:
        - Review of audit processes and procedures.
        - Evaluation of audit work papers and reports.
        - Feedback from audit clients.
        - Monitoring of compliance with the internal audit charter and policy.
- **9.2 External Quality Assessments (if applicable):**
    - External quality assessments may be conducted periodically by a qualified, independent reviewer to provide an objective evaluation of the internal audit function.
    - The frequency and scope of external assessments shall be determined based on regulatory requirements and best practices.
- **9.3 Continuous Improvement:**
    - The internal audit function shall strive for continuous improvement by:
        - Identifying and implementing best practices.
        - Providing training and development opportunities for internal auditors.
        - Monitoring changes in the business environment and regulatory requirements.
        - Seeking feedback from stakeholders.

10. Specific Audit Areas

- **10.1 IT Audit and Cybersecurity:**
    - IT audits shall evaluate the effectiveness of IT controls, including:
        - Data security and integrity.
        - System development and implementation.
        - Cybersecurity risks and controls.
        - Business continuity and disaster recovery.
    - Audits shall assess compliance with relevant IT regulations and standards.
- **10.2 Fraud Risk Management and Investigations:**

- Audits shall consider the risk of fraud and evaluate the effectiveness of fraud prevention, detection, and response mechanisms.
- Internal audit may be involved in conducting or supporting fraud investigations.
- The policy shall align with the organization's overall fraud risk management framework.

- **10.3 Compliance Audit (Regulatory and Legal):**
  - Compliance audits shall evaluate adherence to applicable laws, regulations, and internal policies and procedures.
  - This includes:
    - RBI regulations for NBFC-CICs.
    - Companies Act 2013.
    - Data privacy laws.
    - Anti-money laundering regulations.
- **10.4 Operational Audit (Efficiency and Effectiveness):**
  - Operational audits shall evaluate the efficiency and effectiveness of business operations and processes.
  - This includes:
    - Resource utilization.
    - Process optimization.
    - Performance measurement.
    - Achievement of strategic objectives.
- **10.5 Financial Audit (Accuracy and Reliability):**
  - Financial audits shall evaluate the accuracy and reliability of financial information and the effectiveness of financial controls.
  - This includes:
    - Financial reporting.
    - Accounting policies and procedures.
    - Safeguarding of assets.

11. Policy Review and Updates

- **11.1 Frequency of Review:**

- This policy shall be reviewed and updated at least annually or more frequently as needed.

- **11.2 Amendment Process:**
  - Any amendments to this policy shall be approved by the Audit Committee.
  - The amendment process shall ensure that changes are communicated to all relevant stakeholders.

Annexures

Annexure 1: Risk Rating Guidelines

Depending upon the seriousness and impact of the deficiencies, the audit observations shall be classified under three risk ratings namely, High, Medium and Low.

Appropriate guidelines shall be put in place by Internal Audit Head in discussion and consultation with other functional Heads for assigning such risk grades.

Indicative list of High, Medium and Low risk are given below:

High Risk: The audit report shall be graded as high risk where the audit findings highlight significant matters requiring urgent management action.

Audit findings of the following nature shall result in the internal auditors grading a particular department / operation as high risk:

- A weakness or total failure in the internal control system which presents a grave risk of error that may have a material impact on the financial statements of the Company;
- A weakness where the risk of error, though less likely, involves amounts which may have a major impact on the financial statements;
- A weakness which puts the assets of the Company at jeopardy
- A fraud or suspicion of a fraud.
- Misinterpretation of regulatory guidelines/omission or non- submission of returns and statements or undue delays in submitting them to regulators.

Medium Risk: The audit report shall be graded as medium risk where the audit findings highlight less significant matters requiring management action.

Audit findings of the following nature shall result in the internal auditors grading a particular department/operation as medium risk:

- A weakness in the internal control system which presents a significant risk of error but will not have a material impact
- Deviation of significant nature from the laid down internal policies that had not been ratified/ reported

- Gaps in the process of calculation/ remittance of statutory payments or frequent delays in such payments
- Errors/occasional delays in returns submissions to regulators.
- Improvement relating to the prevailing regulatory environment or procedures which are necessary to avoid minor or technical breaches
- Items pending unreconciled or settled for quite long period
- Customer or investor grievances pending unresolved without valid reasons beyond reasonable period or even after repeated reminders posing reputation risk to the company.
- Loss of income of significant value or visible lax in expenditure

Low Risk: The audit report shall be graded as low risk where the audit findings highlight trivial matters which require to be brought to the attention of the management but do not warrant any immediate action.

Audit findings of the following nature shall result in the internal auditors grading a particular department/operation as low risk:

- Sundry omissions in complying with prescribed policies and procedures of the Company which do not have a material impact on the internal control environment
- Isolated errors and general suggestions relating to efficiency of staff or activity.
- Sundry regulatory related errors which have been rectified and which are unlikely to cause criticism for the regulatory authorities, shareholders and customers
- Deviations from laid down policies due to practical impediments but insulated through compensatory controls duly documented and practiced.

Annexure 2: TAT and Escalation Matrix

S. No	Particulars	TAT	Responsibility
1	Information* Request	3 working days	Auditee SPoC
2	Audit Queries/Observations	3 working days	Auditee SPoC

S.No.	Particulars	Email To	Email Cc
1	T* + 1 working day	SPoC	Head of Department
2	T* + 2 working days	Head of Department	IA Manager at RCAP, SPoC
	T* + 4 working days	Head of Department	CRO of LOB, CEO of LOB, IA Manager at RCAP, SPoC
2	T* + 6 working days	Head of Department, SPoC	Internal Audit Head, IA Manager at RCAP, CRO

Annexure 3: Roles & Responsibilities for Key Activities of Internal Audit

Roles	Responsibilities	Key Activities
Internal Audit Head	Governance	Set Policy & Guidelines, Finalise the Risk Based Audit Plan and Scope, Select Audit Firm & fees finalization, Ensure Completeness of Audit Universe, Ensure Adequacy of Audit Plan and Scope, Ensure adherence to Audit Plan, Prepare Risk Control Matrix (RCM) for the processes being audited, Maintain "No Surprise" environment, Meet with CEO on Annual Plan & Scope and IA Dashboard
"CRO, CFO"	Plan & Scope	Share Key Risks with reference to the Process being audited
Internal Auditor / Audit-In-Charge	Execution	Maintain Appropriate Staffing, Execute Audit following Risk Based Approach, Leverage Data Analytics, Share Best Practices, Timely Reporting
Audit Co-Ordinator	Execution	Prepare draft risk based audit plan and scope and discuss with Internal audit head, Facilitate the audit, Ensure adherence to agreed scope, Obtain Approval for any scope exclusions, Review deliverables. Ensure adequacy of work papers (including Auditor's RCM), Review Audit Document Retention, Ensure Audit Data Confidentiality

Annexure 4: Audit Calendar

S. No	Process Step Description	Output / Record(s)	Period/TAT

1	**Annual Audit Plan**		
1.1	Audit Universe - Maintain a comprehensive list of business units/branches/products/channels/IT Systems/Suppliers	Audit Universe	Draft Dec 31 and Final Mar 31
1.2	Complete a documented risk assessment for each auditable unit (including Map Audit coverage (function/scope/branch) in preceding years 3 years)	Risk Assessment File	Draft Dec 31 and Final Mar 31
1.3	Propose annual audit plan/scope. In case all functions are not proposed to be audited during the year, prepare a multi year plan for the complete coverage	Audit Strategy & Draft Audit Plan	Draft Dec 31 and Final Mar 31
1.4	Finalize the Audit Plan/Scope	Final Audit Plan	April 30 (Based on Audit Committee approval)
2	**Audit process**		
2.1	Audit Execution		As per SOP
	N.B. Cut-off date for Audit		Quarter End minus 1 Month Eg. Audit scheduled in Q3 will cover the period upto Nov 30
2.2	Presentation of Audit Report to Group	Final Audit Report/Presentation	As per SOP
3	**Appointment of External Firm**	IA Services Agreement	April 30 (Based on Audit Committee approval)