

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Reliance Capital Limited

Risk Management Policy

This document is copyright protected in content, presentation, and intellectual origin, except where noted otherwise. You may not modify, remove, augment, add to, publish, transmit, participate in the transfer or sale of, create derivative works from, or in any way exploit any of the elements of this document, in whole or in part without prior written permission from Reliance Capital Ltd. © 2025-2026.

Document Title: Policy Risk Management

Reliance Capital Limited

Originally approved: _____

Last Reviewed: _____

Table of Contents

1. Introduction
2. Risk Management Framework
3. Risk Appetite Statement
4. Risk Governance Structure
 - 4.1. Board of Directors
 - 4.2. Risk Management Committee (RMC)
 - 4.2.1. Composition of RMC
 - 4.2.2. Frequency of Meeting
 - 4.2.3. Roles and Responsibilities of RMC
 - 4.3. Management Risk Committees
 - 4.4. Risk Management Department (RMD)
 - 4.5. Chief Risk Officer (CRO)
5. Risk Management Structure: Three Lines of Defence
6. Risk Identification, Classification, and Policies
 - 6.1. Credit Risk
 - 6.2. Liquidity Risk
 - 6.3. Operational Risk
 - 6.4. Market Risk
 - 6.5. Fraud Risk
 - 6.6. Compliance Risk
 - 6.7. Legal Risk
 - 6.8. Technology Risk
 - 6.9. Collateral Risk
7. Key Risk Appetite Indicators/Thresholds
8. Risk Measurement and Monitoring
9. Stress Testing
10. Risk Reporting
11. Policy Review and Amendments

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

1. Introduction

This policy outlines the framework for managing risks at Reliance Capital Limited (RCL), ensuring alignment with RBI directives, the Companies Act, and other applicable regulations. It aims to provide a structured approach to risk management, protect stakeholder interests, and support the company's strategic objectives.

2. Risk Management Framework

The Risk Management Framework encompasses the policies, processes, controls, and systems used to identify, assess, mitigate, and monitor risks. It is designed to ensure that risk-taking is aligned with the company's risk appetite and strategic goals.

3. Risk Appetite Statement

The Risk Appetite Statement defines the level of risk the company is willing to accept to achieve its objectives. It considers factors like:

- **Risk Culture:** Emphasizes the importance of a sound risk culture where all employees understand their roles in risk management.
- **Capital:** Maintaining adequate capital to absorb unexpected losses and support business growth.
- **Lending:** Managing risks associated with lending activities, including credit quality and concentration.
- **Treasury:** Managing risks related to funding, liquidity, and asset-liability management.

4. Risk Governance Structure

The risk governance structure defines the roles and responsibilities for risk management at all levels of the organization.

- **4.1 Board of Directors:**
 - The Board provides overall governance and oversight of risk management.

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

- It approves the risk management policy and ensures that an effective risk management framework is in place.

- **4.2 Risk Management Committee (RMC):**

The Reserve Bank of India, vide circular DNBS (PD) CC NO. 288/03.10.001/2012-13 dated July 2, 2012, has envisaged the creation of a Risk Management Committee by all NBFCs. This Committee will be responsible for the identification and measurement of risks and also taking suitable measures to prevent the occurrence of such risks.

The RMC is responsible for overseeing the implementation of the risk management framework.

- **4.2.1 Composition of RMC:**

- The RMC includes at least two directors (at least one independent) and the MD.
- The CEO, CFO, and CRO are permanent invitees.

- **4.2.2 Frequency of Meeting:**

- The RMC meets as required, with meetings at least once every 180 days.

- **4.2.3 Roles and Responsibilities of RMC:**

- Approves/recommends risk management policies and strategies.
- Identifies, measures, and mitigates risks.
- Ensures an independent Risk Management Department.

- **4.3 Management Risk Committees:**

- Committees like ALCO and the Credit Committee are responsible for managing specific risk types.

- **4.4 Risk Management Department (RMD):**

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

- The RMD supports business units in implementing risk management policies and monitors risks across the organization.

- **4.5 Chief Risk Officer (CRO):**

Based on the circular DNBR (PD) CC. No.099/03.10.001/2018-19 dated 16 May 2019, RCL has appointed a Chief Risk Officer and following points have been adhered to in this regard:

- The CRO is responsible for the overall development and implementation of the risk management framework.
- The CRO is independent of business functions and reports directly to the RMC.

5. Risk Management Structure: Three Lines of Defence

The company adopts the Three Lines of Defence model:

The 1st Line of Defence will be the Business and Support Units that will own the risks and manage the same, as per laid down risk management guidelines. The primary responsibility for managing risks on a day to day basis will continue to lie with the respective business units of the Company.

The 2nd Line of Defence will be the Risk Management Department that would support the 1st Line of Defence by drawing up suitable risk management guidelines from time to time to be able to manage and mitigate the risks of the Company.

The 3rd Line of Defence will be the Audit Functions – primarily the Internal Audit functions that are supported by External Audits. The 3rd Line of Defence focuses on providing the assurance that the risk management principles/policies and processes well entrenched in the organisation and are achieving the objective of managing the risks of the organization.

6. Risk Identification, Classification, and Policies

The company identifies and classifies risks into the following categories:

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

- **6.1 Credit Risk:**

- The risk of loss due to a borrower's failure to repay a loan.
- Policies include credit appraisal, loan documentation, and portfolio management.

- **6.2 Liquidity Risk:**

- The risk of being unable to meet financial obligations as they fall due.
- Policies include asset-liability management and funding diversification.

- **6.3 Operational Risk:**

- The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.
- Policies include process controls, business continuity planning, and IT security.

- **6.4 Market Risk:**

- The risk of losses in on and off-balance-sheet positions arising from movements in market prices.
- Policies include interest rate risk management and investment guidelines.

- **6.5 Fraud Risk:**

- The risk of losses due to fraudulent activities.
- Policies include fraud prevention, detection, and response.

- **6.6 Compliance Risk:**

- The risk of legal or regulatory sanctions, financial loss, or reputational damage resulting from failure to comply with laws, rules, and regulations.
- Policies include compliance management and monitoring.

- **6.7 Legal Risk:**

- The risk of losses arising from legal actions, inadequate contracts, or lack of legal recourse.

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

- Policies include contract management and legal advisory processes.

- **6.8 Technology Risk:**

- In this digital era, as organizations use information technology (IT) systems to process their information, risk management plays a critical role in protecting an organization's information assets from IT and cybersecurity-related risks. IT risks refer to any type of risks to information technology that can negatively impact the organization's business operations and objectives, whereas cybersecurity risk is the probability of exposure or loss resulting from a cyber-attack or data breach.
- Information technology risks encompass a wide range of potential scenarios such as:
 - - Hardware and software defects, bugs, and system malfunctions, Outages
 - - Regulatory risks
 - - Cyber threats, such as viruses, ransomware, and other types of malwares
 - - Data breaches, data loss, and data theft
 - - Human error
- Common cyber risks in IT systems include but are not limited to:
 - - Ransomware
 - - Data leaks
 - - Phishing
 - - Malware
 - - Insider threats
 - - Phishing attacks
 - - Social engineering attacks
 - - Denial-of-Service attacks.

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Information Technology Risk Management Framework

The practice of risk management within the organization shall be based on impact analysis and risk assessment. The organization shall determine what types of safeguards are appropriate to address their defined risks. The organization cannot, and is not expected to, mitigate every risk, but must prioritize based on the threat to the organization's mission and available resources. The risk management practices implemented by the organization will vary depending upon the nature of the organization's information assets.

Practices that must be included in the organization's risk management program are:

- Discover endpoints and data (desktops, notebooks, servers, mobile devices, and other computer assets).
- Inventory endpoints and data (desktops, notebooks, servers, mobile devices, and other computer assets).
- Categorize the information system (impact/criticality/sensitivity).
- Select and tailor baseline (minimum) security controls.
- Supplement the security controls based on risk assessment.
- Document security controls in the system security plan.
- Implement the security controls in the information system.
- Assess the security controls for effectiveness.
- Authorize information system operation based on mission risk; and,
- Monitor security controls on a continuous basis.
- **6.9 Collateral Risk:**
 - The risk associated with the adequacy and enforceability of collateral.
 - Policies include collateral valuation and title verification.

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

7. Key Risk Appetite Indicators/Thresholds

The policy defines specific metrics and thresholds to monitor key risks, ensuring they remain within acceptable limits. Examples include:

- Credit Risk: NPL ratios, concentration limits.
- Liquidity Risk: ALM mismatches, liquidity coverage ratio.
- Operational Risk: Incident frequency, loss amounts.

8. Risk Measurement and Monitoring

The company employs various techniques to measure and monitor risks, including:

- **Risk Identification and Assessment**

- Identifying and classifying assets within scope.
- Determine the threats and vulnerabilities to the assets, identifying the potential impact of each vulnerability being exploited, and determining the likelihood of occurrence.
- The consolidated information about risk should be maintained in a risk register.

The risk register shall comprise the following minimum components:

- Category
- Risk
- Risk Description
- Impact Description
- Probability Score
- Impact Score
- Inherent Score
- Mitigating Action/Comment
- Compensatory Control
- **Risk Response**

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

Once risk has been assessed, the proper course of action must be determined and implemented. Options include:

- Risk Acceptance – This is a documented decision not to act on a given risk at a given time and place. It is not negligence or “inaction” and can be appropriate if the risk falls within the risk tolerance level.
- Risk Avoidance – These are specific actions taken to eliminate the activities or technologies that are the basis for the risk. This is appropriate when the identified risk exceeds the risk tolerance, even after controls have been applied (i.e., residual risk).
- Risk Mitigation – These are specific actions taken to eliminate or reduce risk to an acceptable level. This is the most common approach and is appropriate where controls can reduce the identified risk.
- Risk Transfer – These are specific actions taken to shift responsibility for the risk, in whole or in part, to a third party. This may be appropriate when it is more cost-effective to transfer the risk, or when a third party is better suited to manage the risk.
- **Risk Monitoring**

RCL must monitor the effectiveness of its risk response measures by verifying that the controls put in place are implemented correctly and operating as intended. This must occur annually, at a minimum. In addition, a process should be defined to monitor significant changes in the factors used to assess the risk (e.g., assets, threats, controls, regulations, policies, risk tolerance). These changes may indicate a new assessment if needed.

Point 4.1.1 & 4.1.2 under Master Direction – Reserve Bank of India (Filing of Supervisory Returns) Directions – 2024 requires the Board and Senior Management shall include the identification assessment and management of data quality as a part of overall risk

Document Title: Policy Risk Management	Reliance Capital Limited
Originally approved: _____	
Last Reviewed: _____	

management framework. All these are sufficiently covered under Cyber security policy of the company.

9. Stress Testing

Stress testing is conducted to evaluate the potential impact of severe but plausible events on the company's financial position.

10. Risk Reporting

Risk reports are provided to the RMC, senior management, and the Board of Directors, covering:

- Risk exposures and trends.
- Compliance with risk appetite.
- Effectiveness of risk mitigation strategies.

11. Policy Review and Amendments

The Risk Management Policy is reviewed and updated at least annually to reflect changes in the business environment, regulatory requirements, and best practices. Any amendments are subject to Board approval.