ARRIBA INCLUSIVE FINANCE PRIVATE LIMITED

RISK MANAGEMENT MANUAL

Table of Contents

Introduction

This document presents the various risk policies of Arriba Inclusive Finance Private Limited (Arriba). These policies have been approved by Arriba's board and are intended to guide informed business decisions. The document covers the following:

1. General Risk Management Policy
2. Operational Risk Policy
3. Credit Risk Policy
4. Liquidity/Funding Risk Policy
5. Interest Rate Risk Policy

These policies will be reviewed by the Board on an annual basis. If necessary, new policies will be formulated to address new risk categories as the organization's operations increase in scale and scope.

1 General Risk Management Policy

1.1 Introduction

Arriba Inclusive Finance Private Limited (Arriba) serves economically underprivileged women by providing them with access to a full range of appropriate financial services. Arriba is a member of the sDevNet.org group of socially-driven institutions, that work closely to provide economic and social services to poor households over a common management and appropriate technology platform.

Arriba's General Risk Management Policy lays down its Risk Appetite as well as the framework of risk management at the organization.

1.2 Adoption

The General Risk Management Policy is approved by Arriba's Board and stated in the sections below.

1.2.1 Categories of Risk

Arriba recognizes the following categories of Risks

- Strategic and Reputation risk
- Operational risk
- Credit risk
- Liquidity risk
- Market risk

It is also to be recognized that risks in different categories impact each other and a good risk management system should take a comprehensive view of the organization.

1.3 Risk Appetite

Arriba's operations will be carried out within the directions and guidelines provided by banking and financial sector regulators such as the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority (IRDA). Arriba will also abide by the laws that may be prescribed by the Government. Those groups of people or businesses engaged in illegal activities will be denied access to services from Arriba.

Subject to the above, the overall risk appetite of the organization will be decided by the Board from time to time and will incorporate the following aspects

1. Minimum rating/assessment grades
2. Maximum annual loss as percentage of Net Worth
3. Capital Adequacy Ratio

1.4 Risk Management Organizational Structure

Board of Directors

The Board of Directors (Board) of Arriba is ultimately responsible for the overall risks of the organization. Responsibilities of the Board include approving risk management policies, defining an overall risk management framework including organizational structure, tolerance limits, and monitoring of the risk profile. The Board will review the status of risks in the organization and will direct the senior management in implementing required policies and controls in the organization.

The Board can delegate the supervision of risks in Arriba to a committee composed of its members. Such a committee of the Board, when formed, should be chaired by an independent director and a majority of its members should either be independent directors or non-executive directors.

Guidelines

- The Board is the only authority that can approve, revise, or cancel policies related to risk management.
- Tasks of the Board include reviewing and approving policies and methodologies, overseeing the organizational structure and delegation of authorities, and reviewing risk reports.
- The Board will define the list of policies that are appropriate for the organization. Such policies will be modified over time and additional policies might be introduced to cover the organization's operations as they expand.
- For each risk category the Board will establish a separate policy. The broad risk categories are 1. Credit Risk, 2. Operational Risk, 3. Liquidity, Funding and Interest Rate Risk and 4. Other Market Risks that may arise in the future (including FX related risks)
- The Board requires reports for all sources of risks produced by various risk owners (department heads). The Board should review the content as well as the structure of these reports.
- The Board will have the right to seek information or report from any department pertaining to any aspect of risk.
- The Board will meet regularly, at least on a quarterly basis.
- Voting Rights: The majority voting rights in the Board on risk management policies will always rest with the Non-Executive Directors.

Management Risk Committee

At the Management level a Management Risk Committee ("MRC") of senior managers will be introduced. The committee will comprise of CEO, Risk Manager and all department heads including heads of the following departments

- Field operations
- Finance, accounts and treasury
- Human Resources
- Administration
- IT and MIS
- Social Performance Management
- Internal Audit
- Risk Management

This MRC is responsible for the daily management of risks within the framework defined by the General Risk Management Policy.

Guidelines

- The MRC should meet on a periodic basis, ideally once every month.
- The MRC should discuss all aspects of risk within the institution. The chair of the MRC rotates among the CEO and other department heads.
- Responsibilities can be allocated to team of managers, for a specified time frame and with clearly defined responsibilities, to look into specific functional areas particularly,
  - Credit
  - Finance (Liquidity, Funding, Interest rate, ALM)
  - Operations
- The Management Risk Committee should establish a reporting structure that captures all risks in the best possible manner. The Board requires cohesive reporting about all risk categories for every Board meeting , and these reports should be produced for review at least 5 working days before each meeting
- A proper escalation mechanism should be established for each risk category so that every employee knows how to react and who to inform in case of a risk-relevant situation

Risk Management Department

In order to facilitate the process of coordination of risks across various departments, a Risk Management Department will be created. The Head of the Risk Management Department will be designated Risk Manager. It is to be recognized that persons responsible for respective functions will continue to remain risk owners.

Guidelines

- Role of the Risk Management department will be to
  - coordinate reporting in the organization along all as risk aspects
  - advise Board about status of risks in the organization
  - report to the Board or its committee and relevant departments if any risk limits or thresholds are breached
  - organise necessary trainings in the organization to instill a sound risk culture
  - periodically assess adequacy of controls in various processes
- The Risk management department will be responsible for making presentations to the Board or its committee in its meetings
- The Risk Manager will report to the Board or its committee and his/her performance will be assessed by the Board

Independent Internal Audit

Arriba will have an Independent Internal Audit function which will receive active guidance from the Board or its committee. Any revision of the contractual terms of the Internal Auditor will be overseen by the Board or its committee. The Head of the Internal Audit department will also be part of the Management Risk Committee. Internal audit reports will be placed before the Board at regular intervals so that the Board has a view on the Internal Control environment within the organization, as assessed by the Independent Internal Audit function.

1.5 Risk Appetite and Limit Structure

Risk Tolerance will be established by Board for the important risks that the organization faces. In order to measure whether risks are within tolerance levels, quantifiable limits should be established for such risks. In case a risk indicator is outside the approved limit, it should be treated as an exception and brought to the notice of the Board. The organization will establish organizational risk appetite and limits for all categories of risks.

1.6 Risk Culture

Risk culture refers to the common beliefs, values and understanding about risks among management, employees, shareholders and board members. Developing appropriate risk culture is an integral part of the Risk Management Framework. The Board of Directors requires the management to develop appropriate risk culture in the organization. This necessitates establishing a healthy and transparent work environment, establishing adequate controls and a system of trainings and dissemination.

Whistle blower policy: In particular, employees who become aware of any violation/breach/misconduct by other employees of the company are expected to bring them to the attention of the company's ombudsperson without any fear of retaliation. The company's ombudsperson will be appointed by the Board. The whistle blower policy will be disseminated widely within Arriba. It should be ensured that each employee of the organization is aware about the right course of action under this policy should s/he find or detect any form of corruption or fraud.

1.7 Key person risk

The Board directs the Management to maintain a list of key persons in charge of critical functions.

In order to ensure smooth and sustainable functioning in case of absence of any of the key persons, a system shall be evolved that ensures that the roles and responsibilities of the key executives can be performed by an identified alternate resource till such time that the key executive returns (or a new key executive joins in).

Given the importance of the responsibilities that the key executives perform, they will have to provide a sufficient notice period of at least two months before they can leave the organization. The notice period can be higher in case the Board is of the view that the time taken to find a suitable replacement will be longer.

Also, the organization will keep ready a succession plan in order to ensure a smooth transition.

2 Operational Risk Management Policy

2.1 Introduction

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Operational risk is inherent in all functional areas of the organization. Poor performance on operational risks can endanger an otherwise perfect risk management framework.

The following broad operational risk areas have been identified by the organization.

1. Internal Fraud – eg. misappropriation of assets including cash, lending to ghost clients, taking bribes from clients, misuse of assets, submitting false expense claims, falsification of information or records
2. External Fraud – eg. theft of information, third-party theft and forgery
3. Employment Practices and Workplace Safety – eg. discrimination, workers' compensation, employee health and safety, staff turnover, staff dissatisfaction
4. Clients, Products, & Business Practice – market manipulation, improper trade, improper staff conduct, unethical practices by competition, problems with products
5. Damage to Physical Assets – eg on account of natural disasters, law and order issues etc
6. Business Disruption & Systems Failures – eg on account of software and hardware failures, disruptive actions of administrative or political establishment, media, community members, etc.
7. Execution, Delivery, & Process Management - data entry errors, accounting errors, failed statutory reporting, loss of client assets through negligence

These risks are caused both by organizational factors as well as by the external factors.

<u>Organizational factors</u>

- Inadequate or unclear policies
- Weaknesses in implementation of processes and controls
- Frauds
- Inadequate training and dissemination
- Failure of IT system
- Errors in planning

<u>External factors</u>

- Regulatory actions
- Activity of competitors
- Natural disasters
- Frauds by external parties
- Administrative and political issues
- Disruptions by media or local communities

Arriba will employ appropriate internal controls to ensure that these risks are within the operational risk appetite of the organization.

2.2 Adoption

The Operational Risk policy of Arriba is approved by the Board and stated in the following sections of this policy document.

2.3 Operational Risk Supervision and Reporting

Board

The Board has the responsibility of developing broad policies for managing operational risks and setting risk tolerance. It also has the responsibility of reviewing status of operational risk at least once in three months. Depending on the requirement, it can order review of critical processes by an external party.

Management Risk Committee

The Management Risk Committee (MRC) of the organization will review the status of operational risks on a monthly basis. The Committee should provide its inputs to the persons responsible for managing operational risk as well as to the Board.

Risk Management Department

The role of Risk Management Department is to coordinate the development of required policies and thresholds, and to ensure that the risks which are not within the set thresholds be flagged and followed-up for their redressal.

Internal audit

Internal audit function of the organization has an important role in management of operational risk. It will review all the processes at periodic intervals to ensure that the controls put in place by the management are working and the will provide status of key processes.

2.4 Risk Identification

Arriba will identify key risks for each of the departments/processes. Primarily responsibility of identification of these risks will be with the respective process owners although they can seek help from the Risk Management department and the Internal Auditor in this. The organization requires respective risk owners to undertake Risk and Control Self Assessment of their respective departments/activities at regular intervals with active involvement of the Risk Management department.

Guidelines

Risk Owners

The key processes at Arriba have been grouped into categories for the purpose of operational risk. The following table presents these processes as well as the process owners.

Process/department	Risk owner
Statutory compliance	CEO
Field Operations	COO
Finance and Treasury	Head - Finance
Process Audit	Head – Internal Audit
Grievance Redressal	Head – Social Performance Management
IT and MIS	Head – IT
MIS – Report Generation	Head – MIS
Human Resource Management	Head – HR

Accounting and Insurance	Head - Accounts
Administration	Head – Admin

All risk owners should perform, with the help of the Risk Management department, self assessment of risks within their respective functions. This assessment should be performed on an annual basis. Results of this assessment should be presented to the Board.

Key Risk Indicators (KRIs)

The operational risk metric has been created to provide an overview of the risks in critical areas. These indicators are expected to help in determining the status of risks in different departments, such as Field Operations, IT, HR, Compliance and Admin. These departments will also be the eventual users of these reports. The risk metric will also be used for management review of overall operational risks during nagement committee meetings. Furthermore, a summary of these reports will be provided to the Board Risk Management Committee. The operational risk indicators along with their frequency of reporting are presented in the table below.

Department	Metric	Frequency
Field Operations	Process Audit Compliance of Branches	Quarterly
Field Operations	Number of Poorly Rated Branches	Monthly
Field Operations	Poorly Rated Branches/Number of Branches	
Field Operations	Client drop-out/Number of Branches	
Field Operations	Client drop-out in Five Branches with Highest Client drop-out/Client drop-out	
Field Operations	Maximum client distance from branch	
Field Operations	Turn around Time	
Field Operations	Client grievances received/Number of Branches	
Field Operations	Client grievances received in Five Branches with Highest grievances/ Total grievances	
Field Operations	Open client grievances > 30 days	
Field Operations	Unscrupulous operators in the field; agents; cases of actions of authorities/politicians/public (not necessarily Arriba's), cases of hate speeches, instigation or rumors against Organization or financial service providers in general	
Field Operations	Cases of unfair practices adopted by competitors – staff/client poaching, staff intimidation, spreading misinformation, rumors, overburdening clients with excessive loans, overheating environment by entering saturated markets and pushing loans where not needed	
HR	Staff dropout/Total Number of Employees	
HR	Number of BMs operating in same branch for two years or more	
HR	Number of Loan Officers operating in same branch for two years or more	
HR	Staff complaints/Total Employees	
HR	Unresolved Staff Complaints > 30 days	
IT	Application downtime (Minutes)	

Department	Metric	Frequency
Various departments	Audit of various branches	

Key Assurances

In addition to the risk metric, Arriba shall evolve a system of assurances for critical functions. These assurances will reflect that important controls are in place and are functioning well. In order to establish the system of assurances, Organization will create process control documents for important processes.

Functions	Key Assurances	Frequency
IT	IT Systems Functionality audit	Annual
IT	IT Systems Performance audit	
IT	IT Security & Stability audit	
IT	IT Open Source compliance audit	
IT	IT Process Documentation audit	
Admin	Infrastructure Status	Quarterly
Admin	Admin Audit Result	
Finance	Covenants of Lenders	
Compliance	Corporate laws	
Compliance	RBI regulations	
Compliance	Labour laws	
Compliance	Fair Practice Code and Code of conduct issues	
Field Operations	Competition	Half Yearly
Field Operations	Regulation	
Field Operations	Law and order Government & Community perspective	

<u>Administration</u>

1. Arriba's operational policy requires the following administration related assurances from the Head, Administration in coordination with the Risk Management department.
   - All insurance related renewals and documentations are in place including,
   - Cash in transit insurance for the branches
   - Fire insurance for the key premises
   - Health and life insurance for all staff
   - Life insurance for the clients and their spouses during the period the loan is active
   - Other insurance as needed
2. All assets at HO and branches are accounted for.
3. Due processes have been followed for all procurement.
4. All critical organizational processes and activities have been documented in the relevant manuals
5. All relevant manuals, circulars and documents are available at the branches/ relevant offices
6. All print material, website is updated and sufficient stationery is available (loan documents, loan cards, receipts, registers, forms, formats etc)

7. All required infrastructure is available and working at HO and all branch offices. No open request for new infrastructure/upgrading or repair is pending over 15 days.

Compliance with Covenants of Lenders

The assurance that Arriba complies with covenants of lenders shall be provided by the Finance department in coordination with the Risk Department. All important lenders covenants applicable to Arriba will be tabulated and compliance with them will be tracked. Some of the important covenants are given below:

Category	Covenant
Financial covenants	• Profitable operations • Status of Portfolio at Risk (PAR) • Capital Adequacy Ratio (CAR)
Inform lender conditions	• Change in capital structure • Further charge on fixed assets • Acquisition of fixed assets • Merger and acquisition • Undertaking guarantee obligations • Borrowings from other lenders
Other conditions	• Utilization of the facility (End use certificate) • Book debt hypothecation (Monthly) • Board approved note on recovery practices • All frauds need to be reported to the banks • Compliance with RBI guidelines • CA certificate on RBI directions

IT and MIS

Arriba's IT head will ensure that key principles of Arriba's unique technologies are always followed. Arriba will exclusively use free and open source technologies, along with technologies supplied by its network technology partner built over the eCubeH Common Appropriate Technology Platform. Fundamental requirements such as completeness of required functionality, high standards of system performance, multi-layered security across the cloud, web & mobile applications and the emerging IoT platform are always maintained. Process documentation for key processes (such as external data sharing relationships with BC banks that have not upgraded yet to open source) should be maintained.

Operational Loss Reporting

The Risk Management department will maintain a database of loss events which will indicate whether the operational risks have materialized. Respective risk owners should provide necessary inputs for maintaining this database. Critical loss events which need to reported are

- Internal frauds
- External frauds
- Theft and robbery
- Law and order issues

- Loss due to natural disasters
- Accidents involving loss of life of staff
- Statutory non-compliance
- Adverse administrative/police/political action
- Unscrupulous finance operators in the organization's operational area

Process and policy manuals

Arriba will prepare and keep updated process and policy manuals for all the departments identified above and address most of the risks identified for the respective processes. These process manuals should be reviewed once annually and should reflect most recent processes. Respective risk owners will provide formal assurance to the Management Risk Committee once annually that the process manuals are up to date in most respects and are being used by the relevant staff.

Risk Based Internal Audit

Internal audit provides an important role in the management of operational risks. All the functional areas of the organization come within the purview of Internal Audit. This function is responsible for checking and reporting whether the specified policies, guidelines and processes are being followed by the organization. The Internal Audit should function independently and should primarily report to the Audit Committee of the Board.

2.5 Risk Tolerance and Limits

In order to ensure that operational risks are within tolerance limits, the Board will establish tolerance limits for critical risk indicators. These will be reviewed periodically. If any indicator is found to be beyond the tolerance limit, it will be reported to the Board.

Guidelines

The management level risk committee should make the Board aware of the critical operational risks. Limits should be proposed for approval by the management committee in a manner that balances operational control with growth objectives.

To start with, limits should be proposed for the following:

1. Losses from frauds, thefts, robberies, accidents, natural disasters.
2. Proportion of poorly rated clients
3. Client drop-out/Number of branches
4. Maximum center distance from branch
5. Staff dropout/Total number of employees
6. Staff complaints/ Total number of employees
7. Unresolved client complaints>30 days
8. Unresolved staff complaints>30 days
9. Total IT application downtime across the organization

2.6 Human Resources

Arriba's policy is to build and maintain an environment that ensures highly motivated and adequately trained employees. It is an equal opportunity employer that rewards performance and promotes an ethical and healthy work culture. Detailed HR guidelines are available in the HR manual. The operational risk policy requires assurances from the HR function in coordination with the risk management department that HR policy guidelines are being followed adequately.

2.7 Outsourcing of key operational processes

Arriba should observe particular caution while outsourcing key processes. The concerned process owner should prepare a note for consideration by the Management Risk Committee for outsourcing specifying rationale, quality and reputation of the vendor, cost implications and potential risks in the outsourcing. The Risk Management department should provide its comments on the note prepared by the respective departments. Final approval to outsource a key process will only be done by the Management Risk Committee.

At least once annually, respective process owners should submit an assurance report to the Management Risk Committee about the outsourced process specifically providing comment on the quality of the service and the business continuity of the vendor.

2.8 Approval for new products, processes

Introduction of a new loan product, significant change in any process or introduction of a new technology will have to be reviewed from the point of view of risk. The concerned risk owner will prepare a note on the risks associated along with the control measures. The Risk Management department will provide critical inputs and suggestions on this. These will be presented in the Management Risk Committee for approval.

2.9 Business resilience and continuity

Respective risk owners must have a standard procedure for ensuring business continuity for limiting losses in case of severe business disruptions. Critical events for which business continuity policy is required will need to be defined by the respective risk owners in consultation with the Risk Management department.

2.10 Training on operational risks

Arriba shall develop appropriate training modules for making staff aware of key risks and their controls. These training programs should ideally be participatory in nature and should include real life case studies from within the organization or from other organizations. The Board encourages such collaborations and reminds all employees and management that the consequences of operational risk events on the profitability and reputation of the organization can be significant.

3 Credit Risk Policy

3.1 Introduction

Credit risk is the risk of loss from non-repayment of loans by borrowers. It is among the most important risks faced by the organization. Arriba's credit risk policy covers its loan products, loan portfolio distribution, delinquency, loan loss provisioning and write-off.

3.2 Adoption

The Credit Risk policy of the organization is approved by the Board as required by the General Risk Management Policy, and stated in the following sections of this policy document.

3.3 Credit Risk Supervision and Reporting

Board

The Board has the responsibility of developing broad policies for managing credit risks and setting risk tolerance. It also has the responsibility of reviewing status of credit risk at least once in three months.

Management Risk Committee

The Management Risk Committee of the organization will review the status of credit risks on a monthly basis. The Committee should provide its inputs to the persons responsible for managing credit risk as well as to the Board.

Risk Management Department

The Risk Management Department should coordinate with the senior credit and operations managers for the development of required policies and limits and to ensure that the risks which are not within the threshold be flagged and followed-up for their redress.

3.4 Risk Tolerance and Limits

In order to ensure that credit risks are within tolerance limits, the Board will establish tolerance limits for important credit risk indicators. These will be reviewed periodically. If any indicator is found to be beyond the tolerance limit, it will be reported to the Board.

Guidelines

The management should make the Board aware of important credit risk indicators. A consolidated report on the following aspects will be shared with the Board every quarter for review:

1. Portfolio at Risk (>0, 30, 60, 90 days) – proportion of portfolio which has overdue for more than 0, 30, 60 and 90 days
2. Portfolio % in Branches receiving poor audit report
3. Hidden delinquency
4. Irregular repayment patterns
5. Portfolio concentration in various geographies and purposes
6. Portfolio concentration in areas prone to natural disasters, communal volatility or other law &

order situation

7. Loan loss provision and write-off – Loan loss provision and write-off as % of portfolio outstanding
8. Rescheduled Loans

Limit Approvals by Board

In order to avoid risk of portfolio concentration, the following exposure limits for the following may be prescribed by the Board. These limits will be reviewed from time to time.

1. Single borrower exposure
2. Exposure to a single district
3. Exposure to a single state
4. Exposure to a single industry
5. Exposure to areas prone to natural disasters, communal volatility or poor in law & order situation
6. Loan portfolio concentration in a single branch
7. Loan portfolio concentration with a single loan officer
8. Loan sizes
9. Loan term

3.5 Policy on Follow-Up of Delinquent Loans

Delinquency is the occurrence of non-payment of even a single loan installment by a borrower. Prompt and regular follow up of delinquent loans is important to ensure sound loan portfolio quality. At the same time, it should be ensured that follow-up of delinquent loan cases is strictly in line with the applicable fair practices directions of RBI as well as Code of Conduct guidelines of industry associations. During follow-up and recovery Arriba's employees shall not use any abusive, violent, or unethical methods of collection.

3.6 Loan Rescheduling

The purpose of rescheduling is to enable the clients to cope with their uncertain cash flow situation and help recover the loan, although it may take more time than originally scheduled. Rescheduling should not be communicated as meaning a waiver of the loans. The CEO will exercise direct authority in determining cases eligible for rescheduling.

Natural calamity, epidemic, accident or civil disturbance (floods, fire, earthquake, riots, arson etc) impacting multiple clients in a group: In situations, where there is loss of earning assets or other property of the clients causing stress on the cash flow of more than two clients, it will be difficult to ensure repayment by invocation of group liability. In such cases, loan restructuring can be considered.

It is to be noted that rescheduling will not impact the MIS and it will continue to show rescheduled cases as overdues in the reports. Each branch will, however, maintain a register of rescheduled cases and file it in the Head Office on a monthly basis.

3.7 Loan Loss Provisioning and Write-Off

The loan loss provisioning and write-off policy will be decided on the basis of the aging of the portfolio, RBI directions as well as expectations regarding loan repayment at Arriba.

4 Liquidity/Funding Risk Management Policy

4.1 Introduction

Liquidity Risk is the risk that the MFI fails to honor its obligations towards clients, banks, investors, and others due to the lack of available funds. Liquidity risk is a particularly sensitive risk category as it has drastic consequences. At any stage, the availability of cash and liquidity should supersede the profitability requirements.

4.2 Adoption

The Liquidity and Funding Risk policy of Arriba is approved by the Board as required by the General Risk Management Policy, and stated in the following sections of this policy document.

4.3 Liquidity Risk Supervision and Reporting

<u>Board</u>

The Board has the responsibility of developing broad policies for managing liquidity risks and setting risk tolerance. It also has the responsibility of reviewing the status of liquidity risk at least once in three months.

<u>Management Risk Committee</u>

The Management Risk Committee of Organization will review the status of liquidity risk on a monthly basis. The Committee should provide its inputs to the persons responsible for managing liquidity risk as well as to the Board.

<u>Risk Management Department</u>

The role of the Risk Management Department is to support the development of required policies and thresholds, and to ensure that the risks which are not within the particular thresholds be flagged and followed-up for their redress. The Finance Manager is the person responsible for overseeing the day-to-day cash and liquidity management as well as debt funds. The Finance Manager will also be responsible for sourcing capital and long term funds.

The Finance Manager needs to ensure that the liquidity position provides a solid basis for the day-to-day business and supports the overall strategic plan. The Risk Manager serves as the independent check point that ensures that funding and liquidity related decisions are in accordance with the organizational policies.

Guidelines

- The Finance Manager is primarily responsible for liquidity related risks, and will monitor such risks in the organization
- Liquidity Risk at Organization is managed through two approaches:

  1. Liquidity Ratio Analysis
  2. Forward-looking Projections

- The Finance Manager should monitor liquidity on a daily basis through day-wise projections of liquidity for the next thirty days. This should include all expected inflows and outflows of cash.
- The Finance Manager should also prepare reports showing the month-wise maturity profile of the outstanding assets and liabilities every quarter.
- The Finance Manager is the highest authority responsible for cash management. S/he may delegate responsibilities to staff members who possess adequate skill and expertise.
- It is the responsibility of the Finance Manager to ensure that required funds are available at the branches as per the scheduled disbursements.
- There will be an information flow from the loan approving body to the cash managing body about current and future payment obligations due to newly approved or renewed loans. This cash outflow needs to be balanced against the cash inflow resulting from interest and amortization.
- The Finance Manager is responsible for the institutional debt-funding of the organization. S/he may delegate the tasks to skilled and suitably qualified staff member but he stays responsible.
- The Finance Manager will attempt to diversify lenders (liquidity providers) so that liquidity is not concentrated with any single source.
- From time to time, the Management Risk Committee will review the number of liquidity providers and whether there is adequate diversification among the sources of liquidity.
- The Risk Manager with help from Finance Manager needs to prepare a funding profile and propose alternative sources of funds as well as their terms & conditions to the CEO.
- This funding profile and the associated responsibilities are part of the discussions of the MRC and the Board.
- The management of the organization at all times will ensure that all lenders' covenants are being complied with. In order to achieve this, the Risk Manager with help from Finance create a list of all covenants. The Finance Manager will check the compliance for all lenders with the respective covenants on a monthly basis.

4.4 Risk Tolerance and Limits

The Board will establish and periodically review tolerance limits for important liquidity risk indicators.

Guidelines

Limits should be established for the following:

1. Projected liquidity gap estimated from the maturity profile of outstanding assets and liabilities
2. Cash and cash equivalents as a proportion of total assets at the end of day
3. Average cash and cash equivalent as a proportion of total assets for a week
4. Cash retained at the branches
5. Capital Adequacy Ratio after factoring in contingent liabilities
6. Debt to Equity Ratio
7. Liquidity Concentration among lenders
8. Proportion of unencumbered assets (that can be sold or securitized) to total assets

4.5 Liquidity Event and Contingency Planning

A liquidity risk event happens when normal business processes cannot be undertaken because of a lack of access to liquid funds. One type of liquidity event is inability to draw cash for disbursement by the organization's branch because of closure of bank due to some unforeseen reason, when disbursements have been planned. There may be other disruptions that may hamper day to day operations. In order to manage such situations, the Risk Manager with help from the the Finance Manager needs to publish and update a table of responsibilities to escalate the matter.

While it is not unusual to have temporary shortfalls in liquidity, an event that can lead to chronic shortage of liquidity for a significant period of time can be catastrophic for the organization. In order to be prepared with an adequate response, should such a situation arise, the Risk Manager with the help of the Finance Manager should periodically carry out liquidity stress tests and prepare contingency plans. Stress test should be performed at least on a quarterly basis.

Guidelines

Liquidity Event Escalation Table

The liquidity escalation table should include the following columns:

1. Liquidity Risk Situations (i.e. situations in which escalations are necessary)
2. Who to address in the case of an escalation (those to be contacted directly as well as those above in the hierarchy who need to be notified of the situation or problem)
3. Function
4. Responsibility in the context of Liquidity Risk Management (this can also be done in an attachment)

Each employee needs to be fully aware of the necessary escalation mechanism including e-mail and phone numbers of the person who needs to be directly addressed as well as each person above in the hierarchy. This is necessary to ensure a well-functioning escalation mechanism.

Stress Tests and Liquidity Contingency Planning

The stress tests should be performed by projecting several scenarios reflecting various risk events for the next one year. These may include:

1. State, sector with highest concentration of loans turning delinquent
2. The lender with the highest loan to the organization recalls its loans
3. Increase in operational expense by 50%
4. Increase in borrowing costs by 50%
5. Worst case scenario where all of the above materialize

Based on the results of the stress test, liquidity contingency plans should be prepared. This should include:

1. Identification of emergency sources of funds including securitization, sale of unencumbered assets etc.
2. Prioritization of operational expenses
3. Prioritization of cash outflows

5 Interest Rate Risk Policy

5.1 Introduction

Interest rate risk is the risk of loss resulting from adverse movements in interest rate. The limited ability to reset interest rates on loans given by the organization in response to increases in its costs of borrowings, gives rise to interest rate risk. Furthermore, as there are regulatory requirements related to Arriba's financial margin (ie the difference between the rate of interest charged on loans and the cost of borrowings from financial institutions and banks), management of interest rate risk is imperative from a regulatory compliance perspective.

5.2 Adoption

The Interest Rate Risk policy of the organization is approved by the Board as required by the General Risk Management Policy, and stated in the following sections of this policy document.

5.3 Interest Rate Risk Supervision and Reporting

<u>Board</u>

The Board has the responsibility of developing broad policies for managing interest rate risks and setting risk tolerance. It also has the responsibility of reviewing status of interest rate risk at least once in three months.

<u>Management Risk Committee</u>

The Management Risk Committee of Arriba will review the status of interest rate risk on a monthly basis.

<u>Risk Management Department</u>

The role of Risk Management Department is to help in the development of required policies and thresholds and to ensure that the risks which are not within the respective thresholds be flagged and followed-up for their redress. The Finance Manager will be responsible for monitoring and reporting interest rate risk.

Guidelines

The monitoring of Interest Rate Risks will be based on the following aspects:

1. Interest rates on assets and liabilities in different buckets defined by interest rate reset dates
2. Loan product wise interest rate

3. Impact on projected profitability for adverse movements in interest rate
4. Regulatory guidelines

Reports relating to the aspects identified above will be prepared on a monthly basis by the Finance Manager or a person designated by him/her. These reports will be discussed in Management Risk Committee meetings. In these meetings the following will be reviewed.

Adherence to regulatory guidelines

Adherence to interest rate and margin cap regulations will be reviewed.

Pricing (Interest rate) gaps

Variable rate borrowings and particularly pricing or interest rate gaps should be carefully monitored. Liabilities should be grouped in monthly buckets reflecting dates of reset of their interest rates. Due to the constraint that the organization cannot retrospectively reset the interest rate on loans that have been disbursed, the amounts in each bucket reflects pricing gaps.

Lending rates

Based on the interest rate risk reports, interest rates charged on the loan products will be reviewed and if necessary changed in line with the limits set by the Board (discussed below).

Borrowing rates

Similarly, decisions related to liabilities will be reviewed. If it is found that the cost of new liabilities that can be realistically accessed by the organization exceeds the limits approved by the Board (discussed below), then a board approval shall be sought for making these borrowings.

Impact on profitability

Increase in borrowing rates can reduce the profitability of the organization. During the monthly review committee meetings, the impact of changes in the borrowing rates should be discussed.

Scenario analysis and stress tests

Scenario projections and stress tests are required by the Interst Rate Risk Policy of the organization. The interest rate policy requires that these scenarios should include scenarios involving high interest rates.

5.4 Risk Tolerance and Limits

The Board will establish and periodically review tolerance limits for important interest rate risk indicators.

Guidelines

Lending rates on products: The Board will approve the lending rates on loan products as well as the extent to which they can be changed in the next quarter

Borrowing rates: The Board will approve the maximum rates at which the organization can borrow funds in the next quarter. Any borrowings, the cost of which exceed the approved rates, will have to be approved by the Board.

Net Interest Margin (NIM): The NIM will be in accordance with RBI directions on margin caps.

Interest rate caps: Interest rate cap (if any) will be in accordance with the RBI directions.