

THE BIHAR STATE CO-OPERATIVE BANK LTD.PATNA
ASHOK RAJPATH-800004



RISK MANAGEMENT POLICY

(DATE:-02-11-2021)

Contents

<i>Sr. No.</i>	<i>Particulars</i>	<i>Page No.</i>
1	Introduction	3
2	Credit Risk	11
3	Liquidity Risk	32
4	Market Risk	37
5	Operational Risk	42
6	Compliance Risk	56
7	IT Risk	62
8	Abbreviations Used	68

1. Introduction

Risk is an integral part of the banking business and aims at delivering superior shareholder value by achieving an appropriate trade-off between risk and returns. Risk management strategy is based on a clear understanding of various risks, disciplined risk assessment and measurement procedures and continuous monitoring. The key risks which a bank faces are credit risk, market risk and operational risk. The policies and procedures established for minimizing these risks are continuously benchmarked with best practices.

(i) Need for Risk Management in the bank

The bank has put forward this document for the purpose of providing guidelines on minimum requirements for risk management system. For the purpose of these guidelines, all risks in the bank are the possibility that the outcome of an action or event could bring about adverse impacts on the bank's capital or earnings. Such outcomes could either result in direct loss of earnings/capital or may result in imposition of restrictions on bank's ability to meet its business objectives.

(ii) Objectives of Risk Management Policy

The overall purpose of the risk management policy is to evaluate the potential losses for the bank in the future and to take precautions to deal with these potential problems when they occur. The main objectives of the Risk Management Policy are:

1. To ensure that all the current and future material risk exposures of the bank are identified, assessed, quantified, appropriately mitigated and managed.
2. To establish a framework for the bank's risk management process and to ensure bank wide implementation.
3. Protect the financial assets, physical assets, reputation, and interest of the members of the bank.
4. To enable compliance with RBI/NABARD regulations and guidelines and internal policies through the adoption of best practices.
5. Assist in fulfilling the cooperative principles.
6. To assure business growth with financial stability.

The bank will align all its policies including loan, investment, ALM, KYC, I.T. policy to Risk Management Policy. All policies including the bank's risk management policy shall be reviewed/ updated once in two years. The bank will regularly review risk management approaches to better understand and manage bank's exposure to risks within risk appetite.

(iii) Coverage of the Risk Management Policy: - This policy covers the following riskcategories:

1. Financial Risk

- a) Credit risk
- b) Liquidity risk
- c) Market risk
 - i. Interest rate risk
 - ii. Foreign exchange risk
 - iii. Equity risk
 - iv. Commodity risk

2. Non-Financial Risk

- a) Operational risk
- b) Compliance risk
- c) IT risk

1. Financial Risk

- a) Credit Risk:** - Credit risk is the current or prospective risk to the earnings and capital arising from the customer's failure to meet the terms of any contract with the bank or if the customer otherwise fails to perform as agreed. Credit risk can be small or big depending on the size of the portfolio and volume of the exposure to the segment by the bank.
- b) Liquidity Risk:** - Liquidity risk is the potential inability to generate cash or have access to liquid assets to cope with deposit withdrawals, payment commitments or fund increase in business. This risk arises due to mismatches in maturity pattern of assets and liabilities, mainly in short term.
- c) Market Risk:** - Market risk is the risk that the value of on and off-balance sheet positions of a bank/ financial institution will be adversely affected by movements in market rates or prices such as interest rates, foreign exchange

rates, equity prices, credit spreads and/or commodity prices resulting in a loss to earnings and capital.

2. Non-Financial Risks

- a) Operational Risk:** - Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. It seeks to identify why a loss happened and at the broadest level includes the breakdown by four causes: processes, people, systems, and external factors.
- b) Compliance Risk:** - Compliance risk is the current or prospective risk arising from violations or non-compliance with laws, rules, regulations, agreements, prescribed practices, or ethical standards, as well as from the possibility of incorrect interpretation of effective laws or regulations. Non-compliance with the legal and regulatory and other orders could result in financial losses on account of penalties, etc.
- c) IT Risk:-** The motive of Information Technology risk management is to assist bank to establish an effective mechanism that can identify, measure, monitor, and control the risks inherent in bank's IT systems, ensure data integrity, availability, confidentiality, and consistency and provide the relevant early warning mechanism.

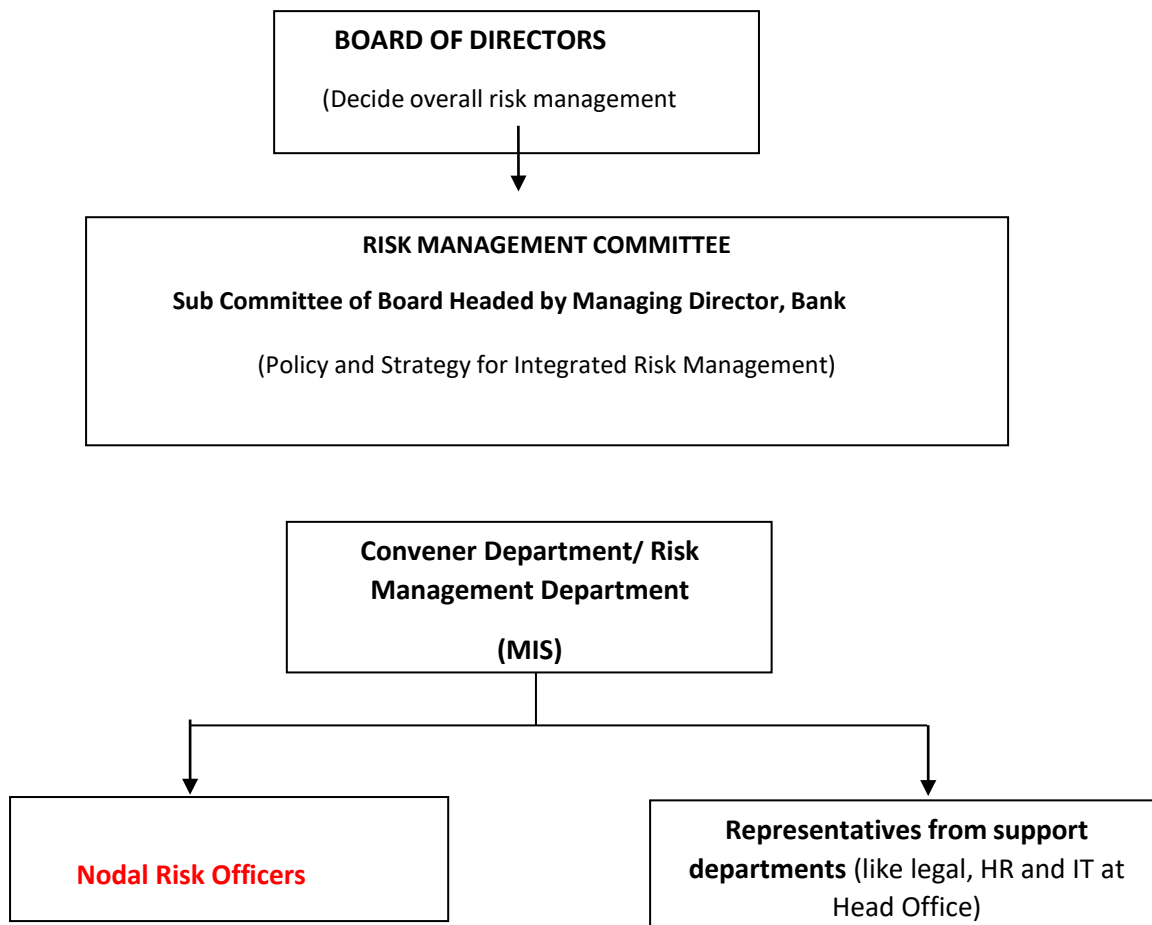
(iv) Risk Management Framework

For successful implementation of risk management framework, it is essential to nominate senior management individuals to lead the risk management teams. Periodic workshops must be conducted to ensure awareness of the policy and the benefits of following them. This will ensure that risk management is fully embedded in management processes. Senior management involvement will ensure active review and monitoring of risks on a constructive 'no-blame' basis.

The board of directors, through the bank's risk management committee, will be responsible for risk oversight. This includes reviewing and approving risk management policies, risk exposures and limits, whilst ensuring the necessary infrastructure and resources are in place.

For overseeing the effective Risk Management function in the bank, the bank will constitute "Risk Management Committee" and the organizational set-up for Risk Management shall include the following:

a) Organizational Structure for Risk Management:-



1. Risk Management Committee Structure:-

RISK MANAGEMENT COMMITTEE:-

- I. MANAGING DIRECTOR-AS A CHAIRMAN
- II. THREE DIRECTOR NOMINATED BY BOARD
- III. HEAD OF CREDIT, INVESTMENT, AUDIT, COMPLIANCE, OPERATIONAL RISK, ETC
- IV. HEAD OF IT DEPARTMENT WILL BE SPECIAL INVITEE.

(i) Roles and Responsibility of Board of Directors & Management:-

a) Board of Directors

- 1. Approve and periodically review the Risk Management framework and Risk Policy.
- 2. Approve the Bank wide risk tolerance; review the Bank's exposure to its key Risks.
- 3. Assess the effectiveness of risk mitigation plan implemented by the Bank to manage all Risks.
- 4. Provide strategic guidance on various initiatives undertaken by the Bank

towards management and mitigation of all Risks.

b) Risk Management Committee (RMC)

1. Risk Management Committee (RMC) will be primarily responsible for ensuring effective management of all Risks in the Bank.
2. Review various Risk related issues and incidents and focus on important issues requiring attention at the policy or process level.
3. Review the risk profile, understand future changes and threats, and prioritize action steps.
4. Review and approve the development and implementation of Risk methodologies and tools, including assessments, reporting, etc.
5. Monitor and oversee the implementation of the Risk Management framework in the Bank.
6. Review the results of 'root cause analysis' of loss events and approve changes in the internal control mechanism.
7. Approve risk capital methodology.

c) Quorum and mandatory members

Quorum will be a minimum of SIX members with Managing Director, as Chairman, in the absence of MD, General Manager/DGM (Admin) will act as Chairman of the meeting. In the absence of both, General Manager/DGM (Accounts) will act as Chairman of the meeting and the convener department being mandatory.

The committee shall be assisted by the staff possessing requisite skills and they would be trained periodically.

d) Risk Management Department (RMD)/Convenor Department (MIS)

1. Under the leadership of the CRO/DGM, RMD the department supports the Board and the Risk Management Committee in management of the Risk Management Framework and setting of the relevant Risk Management Policies and Risk Appetite / Tolerance limits.
2. Responsible for developing and updating the risk management framework of the bank and related policies, procedures, and methodologies.
3. Based on the framework and policies, the RMD is responsible for coordinating the

process to identify, measure, control or mitigate, treat, monitor, and report on risk exposures.

4. Coordinate the development of Business Continuity Plan which is ready to invoke in response to natural or man-made events that may lead to business interruption and/or losses to the Bank.
5. Supporting management to inculcate a Risk Culture throughout the Bank.
6. Coordinate and provide technical support to the business units with respect to risk management and check that the Risk Management Policy is properly implemented.

e) Chief Risk Officer (Convener of RMC)

1. Deputy General Manager of Convener Department is Chief Risk Officer of the Bank.
2. To coordinate meeting of RMC at least once in a half year or earlier, as and when required.
3. All key risks identified shall be documented in the Consolidated Risk Register maintained at convener department will be authenticated by Chief Risk Officer.
4. To monitor the mitigation plan for the risks identified in the consolidated risk register and place it for review of Risk Management Committee in the meeting.
5. To circulate Agenda for the RMC meeting.
6. To attend all RMC meetings.
7. To maintain Minutes of all RMC meetings
8. To propose periodic updates in risk management policy.
9. To facilitate the analysis of risks and interrelationships of risks across credit, market, and operational risks.
10. He will be a member of all Risk Management Committees viz., Credit Risk Management Committee, ALCO, Operational Risk Management Committee, Inspection Committee, Capital Planning Committee and Committee of Executives on fraud risk reporting and management.
11. He will also present the memorandum relating to Risk Management to Risk Management Committee, Board of Directors, ALCO and Audit Committee of the Board and Special Committee of the Board for large value frauds.
12. Create and promote risk awareness across all members of the Circle/Region.
13. Ensure that all the branches are carrying out the responsibility relating to risk management.

14. Evaluate the risk and mitigation plan recommended by branch heads.
15. Direct branch heads for mitigating the risks identified.

f) Monitoring and Review

The Policy shall be reviewed once in two years or more frequently if there is a major change to the Bank's risk management framework. Changes to the Policy must be approved by the Risk Management Committee before seeking approval of the Board of Directors. Structured agenda covering credit risk, market risk, operational risk, compliance risk and other risks impacting the bank will be placed before the committee for discussions and follow-up action.

Financial Risks

- ❖ **Credit Risk**
- ❖ **Liquidity Risk**
- ❖ **Market Risk**
 - **Interest Rate Risk**

1. Introduction

Banks are exposed to credit risk as and when banks' funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether recorded on the Banks' balance sheet or off the balance sheet.

Credit risk refers to the risk that a borrower will default on any type of debt by failing to make required payments. Or Credit risk is most simply defined as the potential that a bankborrower or counterparty will fail to meet its obligations in accordance with the agreed terms. Credit risk may also arise in the situation where the performance of guarantors is required to fulfil the debt obligation.

Credit risk or default risk involves inability or unwillingness of a customer or counterparty to meet commitments (with agreed terms) in relation to lending, trading, hedging, and other financial transactions. Credit risk, therefore, arises from the banks' dealings with or lending to a corporate, individual, another bank, financial institution, or a country.

Banks are increasingly facing credit risk (or counterparty risk) in various financial instruments other than loans, including acceptances, interbank transactions, trade financing, foreign exchange transactions, bonds, equities, and in the extension of commitments and guarantees, and the settlement of transactions. The Credit Risk is generally made up of transaction risk or default risk and portfolio risk.

Credit risk may take various forms, such as:

- **in the case of direct lending**, that funds will not be repaid as per agreed terms,
- **in the case of guarantees or letters of credit**, that funds will not be forthcoming from the customer upon crystallisation of the liability as per the contract,
- **in the case of treasury products**, that the payment or series of payments due from the counterparty under the respective contract is not forthcoming or
- **in the case of securities trading businesses**, that settlement will not be affected,
- **in the case of cross-border exposure**, that the availability and free transfer of currency is restricted or ceases

The risk is primarily that of the bank (lender) and includes lost principal and interest, disruption to cash flows, and increased realisation costs. The loss may be complete or partial and the collaterals provided to the bank do not cover the bank's claims.

2. Types of Credit Risk

1. Credit default risk

The risk of loss arising from a debtor being unlikely to pay its loan obligations in full or the debtor is more than 90 days past due on any credit obligation, default risk may impact all credit-sensitive transactions, including loans, securities, and derivatives.

2. Concentration risk

The risk associated with any single exposure or group of exposures with the potential to produce large losses to threaten a bank's core operations. It may arise in the form of single name or group or inter-connected party concentration or industry concentration.

3. Country risk

The risk of loss arising from a sovereign state freezing foreign currency payments (transfer/conversion risk) or when it defaults on its obligations (sovereign risk), this type of risk is prominently associated with the country's macroeconomic performance and its political stability.

Credit Risk at BSCB

Credit risk is bank's main financial risk. Most of the credit risk arises in the Bank's lending operations. **The Bank is also exposed to credit risk in its treasury activities. Despite a reasonably well-diversified portfolio, the Bank is subject to concentration risk due to its regional focus, i.e., in the state of Bihar, and major lending to agriculture sector.**

Credit Risk Management in the Bank

The goal of credit risk management is to maximise a bank's risk-adjusted rate of return by maintaining credit risk exposure within acceptable parameters. Bank will manage the credit risk inherent in the entire portfolio as well as the risk in individual credits or transactions. The bank's comprehensive credit risk management policy will address these six areas,

- i. Establishing an appropriate credit risk environment

- ii. Operating under a sound credit granting process
- iii. Maintaining an appropriate credit administration, measurement, and monitoring process
- iv. Credit risk assessment
- v. Credit Risk Mitigation and
- vi. Role of Board of Directors and Senior Management

These practices will also be applied in conjunction with sound practices related to the assessment of asset quality, the adequacy of provisions and reserves, and the disclosure of credit risk, as addressed in Basel Committee documents and RBI/NABARD regulations and guidelines.

1. Credit Risk Environment

The board of directors should have responsibility for approving and periodically (at least once in two years) reviewing the credit risk strategy and significant credit risk policy of the bank. The strategy should reflect the bank's tolerance for risk and the level of profitability the bank expects to achieve for incurring various credit risks.

Senior management should have responsibility for implementing the credit risk strategy approved by the board of directors and for developing policies and procedures for identifying, measuring, monitoring, and controlling credit risk. Such policies and procedures should address credit risk in all the bank's activities and at both the individual credit and portfolio levels.

Bank should identify and manage credit risk inherent in all products and activities. Bank should ensure that the risks of products and activities new to them are subject to adequate risk management procedures and controls before being introduced or undertaken and approved by the board of directors.

2. Credit Granting (Sanction) Process

Credit assessment and granting process

Credit granting includes – origination, assessment, and sanction.

Bank must operate under sound, well-defined, effective, and efficient credit-granting process as per the Loan Policy of the Bank. The credit granting criteria should set out

who is eligible for credit and for how much, what types of credit are available, and under what terms and conditions the credits should be granted.

These criteria should further include:

- a thorough understanding of the borrower or counterparty,
- understanding the purpose and structure of the credit, and its source of

repayment. Bank must ensure that:

- there are well defined and clear eligibility norms and processes for credit appraisal,
- credit-granting function is being effectively managed,
- the credit exposures are within levels consistent with prudential standards and internal limits,
- systems to assign a risk rating to each customer/borrower (above a certain limit) to whom credit facilities have been sanctioned,
- credit rating mechanism to price credit facilities depending on the risk grading of the customer,
- that exceptions to policies, procedures and limits are reported in a timely manner to the appropriate level of management for action,
- the staff involved in credit sanction/ review/ renewal activities are fully capable, experienced, and trained for conducting the loan activity to the highest standards and in compliance with the bank's policies and procedures,
- bank imparts training to officers dealing with credit from time to time.

Delegation of credit sanctioning authority to various levels including board committees, senior management, and staff (including authority to approve deviations and exceptions), is well documented and strictly followed.

Reporting procedures of sanction of credit of various committees at HO level and branch managers, as documented in Loan Policy of the Bank, are strictly followed.

Depending on the type of credit exposure and the nature of the credit relationship, the following factors documented in loan policy for approving credits are considered while sanctioning credit limits:

- the purpose of the credit and sources of repayment,
- the current risk profile (including the nature and aggregate amounts of risks) of the borrower or counterparty and available collateral security,

- the borrower's repayment history and current capacity to repay, based on historical financial trends and future cash flow projections, under various scenarios,
- for commercial credits, the borrower's business expertise,
- the proposed terms and conditions of the credit, including covenants, and
- where applicable, the adequacy and enforceability of collateral or guarantees, including under various scenarios.

Credit Concentration and Credit Exposure limits as per RBI and CMA norms defined by NABARD

- The bank shall have sound and well-defined policies and procedures incorporating credit concentrations limits to ensure that credit activities are adequately diversified.
- The policy on large exposures shall be well documented in bank's Loan Policy document, to enable the bank to take adequate measures to ensure that concentration risk is limited.

The bank will monitor the exposure levels carefully such that the limits are not breached. An appropriate MIS about this issue will be created for the board review.

The following RBI guidelines on Managing Credit Risk should be scrupulously followed:

- Not to grant loans against security of its own shares
 - Remission of debts for other Cooperative Banks without prior approval of RBI
 - Follow restrictions on loans and advances to Directors and their relatives**
 - To observe ceiling on advances to Nominal Members – With deposits up to 50 crore(50,000/- per borrower) and 1,00,000/- for above 50 crore.
 - Not to sanction bridge loans including that against capital / debenture issues
 - Bank not to extend any facilities to stock – brokers.
 - Loans under Real Estate Sector to be provided only for genuine construction and not for speculative purposes.
- ☒ Not to lend more than 15% of **Tier -I capital** to individual borrower#
- Not to lend more than 25% of **Tier – I capital** to a group of borrowers# The bank shall have at least 50 per cent of their aggregate loans and advances comprising loans of not more than ₹25 lakh or 0.2% of their Tier I capital, whichever is higher, subject a maximum of Rs.1 crore, per borrower/party.

RISK MANAGEMENT POLICY

*** (amended by RBI circular RBI/2020-21/89 dated the February 5, 2021, as under:*

Cooperative Banks shall not make, provide, or renew any loans and advances or extend any other financial accommodation to or on behalf of their directors or their relatives, or to the firms / companies / concerns in which the directors or their relatives are interested (collectively called as “director related loans”).

Further, the directors or their relatives or the firms / companies / concerns in which the directors or their relatives are interested shall also not stand as surety/guarantor to the loans and advances or any other financial accommodation sanctioned by Cooperative Banks.

‘Advances’ for the purpose shall include all types of funded / working capital limits such as cash credits, overdrafts, credit cards, etc).

The following categories of director-related loans shall, however, be excluded from “loans and advances” for the purpose of these directions:

- i. Regular employee-related loans to staff directors, if any, on the Boards of Cooperative banks.*
- ii. Normal employee-related loans to Managing Directors / Chief Executive Officers of Cooperative banks.*
- iii. Loans to directors or their relatives against Government Securities, Fixed Deposits and Life Insurance Policies standing in their own name.)*

(Reduced from 40% to 25% by RBI, Circular No. RBI/2019-20/171 dated the March 13, 2020, capital funds have been replaced with Tier – 1 capital).

(The revised exposure limits shall apply to all types of fresh exposures taken by the bank. Bank shall bring down their existing exposures which are in excess of the revised limits to within the aforesaid revised limits by March 31, 2025. However, where the existing exposure comprises only term loans and non-fund-based facilities, while no further exposure shall be taken on such borrowers, these facilities may be allowed to continue as per their respective repayment schedule / till maturity).

Sanction of Credit Limits beyond the Exposure Limit:

Prior Authorization from NABARD to be obtained for lending by the Bank beyond Certain Limits and to Certain Categories of Borrowers.

i). The bank shall obtain prior authorization of NABARD for sanction of credit limits by the bank on its own or in consortium with other banks to the following categories of borrowers, where the aggregate amount of sanction is beyond the prescribed cut-off

limits:

- I. Cooperative marketing societies
- II. Consumer stores societies
- III. State level cooperative federations in respect of purchase / procurement schemes of the State Government (other than food credit)

ii) The bank shall obtain prior authorization of NABARD for financing State level Marketing Federations for procurement of food grains at Government support price on commercial basis outside PDS where the aggregate amount of sanction is beyond the cut-off limits as prescribed by NABARD from time to time.

Inter-Bank Exposure limit

The interbank exposure is applicable in terms of market operations, investments, and treasury operations, and are covered in detail in the Investment Policy of the Bank duly approved by the Board.

Approving Large credits for first time

In approving large credits – over a limit of Rs. 25 lakhs – to borrowers or counterparties for the first time, consideration should be given to the integrity and reputation of the borrower or counterparty as well as their legal capacity to assume the liability. Prior to entering any new credit relationship, the bank must be confident that they are dealing with an individual or organisation of sound repute and credit worthiness.

A comprehensive assessment of the risk profile of the customer will include the purpose of the loan, repayment sources, financial statements, integrity and reputation of the borrower or counterparty.

Bank may introduce a Loan Appraisal Committee (LAC) at Head Office (with senior officers from Loan, Planning, Risk Management, Credit Monitoring & Recovery department) for granting “in principle” approval to a new business connection above a limit of Rs. 25 lakhs. Only after this approval, the proposal may be accepted for processing and sanction.

Once new credit connection is approved “in principle”, it is essential for the bank to ensure that the information received from the applicant is sufficient to make proper credit-granting decisions. This information will also serve as the basis for rating the

credit under the bank's internal credit rating system.

Analyse Non-financial Risks in case of large borrowers (over a limit of Rs. 25 lakhs)

In addition to financial risks assessment including creditworthiness, qualitative criteria such as management, competitive situation, and market position (local competitors, market share, competitiveness of services,) industry, etc. should be assessed qualitatively.

Know Your Customer

Know your customer (KYC) is an integral part of the credit risk management process and forms the basis for all subsequent steps in the lending process. This involves mandatory verification of new and existing customers' credentials to prevent money laundering. Strict policies must be in place and followed to avoid association with individuals involved in fraudulent activities and other crimes.

Policy Relating to Credit Products

- Bank shall maintain adequate documentation relating to various types of loan products.
- New credit products must be introduced after a careful review of the existing and potential risks inherent in the products.
- The pricing of these products should be included and periodically reviewed.
- Prior approval for all new products shall be obtained from the Board after their clearance from Risk Management Committee.
- All material risks arising from new products shall be assessed before introduction to customers.
- All credit products introduced by the bank should be periodically reviewed based on their performance and achievement of objectives of introducing such products.
- If possible, the expiry date of product may be specified.

➤ Credits to Related Companies and Individuals

Credits to related companies and individuals must be authorised on an exception basis, monitored with particular care and other appropriate steps taken to control or mitigate the risks.

Extension of credit to directors, management, and other influential members, should be as per the established credit granting and monitoring processes.

Unsecured Exposure

Unsecured exposure is an exposure comprising all funded and non-funded exposures (including underwriting and similar commitments) where the realisable value of security, as assessed by the Bank/ approved valuers/ Reserve Banks Inspecting Officers, is not more than 10 percent, ab-initio, of the outstanding exposure.

But the classification of advances as secured or unsecured should be revisited at the time of review of advances and also as part of preparation of final statements.

Security will mean tangible security properly charged to the Bank and will not include intangible securities like guarantees (including State Government Guarantees), comfort letters, charge on rights, licenses, authorisations etc.

Unsecured advances shall include clean overdrafts, loans against personal security, clean bills or Multani hundies purchased or discounted, cheques purchased and drawals allowed against cheques sent for collection.

As per RBI guidelines, Cooperative Bank, whose priority sector loan portfolio is not less than 90% of the gross loans may grant unsecured advances to the extent of 35 % of their total assets as per the audited balance sheet at the end of the preceding financial year, subject to the following conditions:

- a. The entire unsecured loan portfolio in excess of the normally permitted 10%, shall comprise of priority sector loans and the exposure to any individual borrower shall not exceed ₹ 40,000/-.
- b. The bank complies with the eligibility criteria of:
 - i. CRAR of not less than 9%.
 - ii. Gross NPAs of not more than 7%.

Credit Administration, Measurement and Monitoring Process

Credit Administration

The bank shall have a system for the on-going administration of its various loans accounts. The internal auditors and concurrent auditors (wherever applicable) will ensure that loan portfolios are properly maintained and administered. This will include record keeping, preparation of the terms and conditions as well as perfection and safe

custody of the securities. Credit files shall, at a minimum, contain the following information:

- i. Loan application
- ii. Evidence of sanction with terms and conditions
- iii. Acceptance of terms and conditions by counter party
- iv. Latest financial information
- v. Record of dates of all credit reviews and renewals
- vi. Record of all guarantees and securities
- vii. Evidence of securities validation function including legal validity (legal opinion and non - encumbrance report by bank empaneled advocate), existence (physical verification report), valuation (valuation report by bank empaneled valuer), registration of charge and safekeeping.
- viii. Credit score report of CIBIL or any other similar agency approved by the bank.

Loan Review/ Renewal Mechanism

Loan review/ renewal shall take place in each and every loan facility once in a year. In case submission of financial statements and other information is delayed by the borrower, the bank shall undertake a “ad-hoc/ short review” of the account based on the conduct of account, available information and compliance status of terms and conditions of sanction. Such “ad-hoc/ short review” shall not be valid for more than **THREE** months.

Timely and comprehensive review/renewal of credit facilities should be an integral part of the Board approved loan policy and credit risk management framework, and banks should avoid frequent and repeated ad-hoc/short review/renewal of credit facilities without justifiable reasons. Banks are also advised to capture all the data relating to regular as well as ad-hoc/short review/renewal of credit facilities in their core banking systems/management information systems and make the same available for scrutiny as *and when required by any audit or inspection by Auditors/RBI. Further, the processes governing review/renewal of credit facilities should be brought under the scope of concurrent/internal audit/internal control mechanism of banks with immediate effect.*

As per RBI circular No. RBI/2020-21/27 dated the August 21, 2020, on Ad-hoc/Short Review/Renewal of Credit Facilities and when required by any audit or inspection by Auditors/RBI. Further, the processes governing review/renewal of credit facilities should be brought under the scope of concurrent/internal audit/internal control mechanism of banks with immediate effect.

Unquote

The main objectives of Loan Review Mechanism could be: ·

- i. to identify promptly loans which develop credit weaknesses and initiate

- timely corrective action, ·
- ii. to evaluate portfolio quality and identify potential problem areas, ·
 - iii. to provide information for determining adequacy of loan loss provision, ·
 - iv. to assess the adequacy of and adherence to, loan policies and procedures,
 - v. to monitor compliance with relevant laws and regulations, and ·
 - vi. to provide senior management with information on credit administration, including credit sanction process, risk evaluation and post-sanction follow-up.

Watch listed Exposure

After the identification of a seriously deteriorated debt repayment capacity and/or a serious deterioration in the financial standing, the counterparty is placed on the watchlist and becomes subject to specific watch-list monitoring. The Credit Committee decides on the watch-listing of all loans, borrowers, and Treasury counterparties.

Watch-listed counterparties are reviewed by the Credit Committee at agreed intervals and reported to the Board of Directors.

Dealing with Problem Credits

- Early recognition of weaknesses in the credit portfolio is important and allows for effective determination of loan loss potential.
- The bank must have clearly articulated and documented policies in respect of past due credit facilities and shall at a minimum have approval levels and reporting requirements in respect of granting extensions, deferrals, renewals, and additional credit facilities to existing accounts.
- The policy shall define a follow-up procedure for all loans and identify the reports to be submitted both to senior management and board of directors

Measurement of Credit Risk

As per RBI guidelines, measurement of Credit Risk could be:

1. Through Credit scoring / Credit

Credit rating is done with primary objective to determine whether the account after the expiry of a given period will be able to meet its obligation to its creditors, including bank and would not be in default.

2. Quantifying risk through estimating loan losses:

The amount of loan losses that bank would experience over a chosen time horizon (through tracking portfolio behaviour over 5 or more years) and unexpected loan losses i.e., the amount by which actual losses exceed the expected loss (through

standard deviation of losses or the difference between expected loan losses and some selected target credit loss quintile)

3. Risk pricing – Base lending rate which also accounts for risk.

4. Risk control through effective Loan Review Mechanism and Portfolio Management.

The measurement of credit risk should consider:

- i. the specific nature of the credit, maturity, exposure profile, existence of collateral or guarantees and potential for default and environmental circumstances and its contractual and financial conditions
- ii. the existence and value of security (collateral or guarantees), and
- iii. the potential for default based on the internal risk rating.

The bank can have procedures for measuring its overall exposure to credit risk including exposure to related parties, products, customers, market segments and industries for appropriate risk management decisions to be made.

The analysis of credit risk data should be undertaken at an appropriate interval (monthly/ quarterly/ half- yearly) with the results reviewed against relevant limits.

Monitoring of Credit Risk

The Bank puts strong emphasis on continuous monitoring of the credit risk in its lending and treasury operations. Credit risk is monitored both at counterparty level and at portfolio level.

The primary responsibility for credit risk monitoring resides with the functionaries (branches and regional offices) responsible for the client relationship. Risk Management Department is responsible for regular reporting to the Board of Directors and Senior Management on the Bank's risk position in relation to established limits.

Monitoring credit exposures

All credit exposures are subject to continuous monitoring. As per Loan Policy, an annual review/ renewal is conducted on the entire loan portfolio. The annual review/ renewal includes a follow-up of the customer relationship, compliance of sanctioned terms and conditions, conduct of account, as well as a credit risk review.

All exposures are subject to continuous monitoring of events/ identifying early warning signals (EWS) / Red Flags, that could potentially lead to or indicate a

material change in risk. Monitoring of compliance with limits for counterparty credit exposure is carried out by Risk Management Department on a daily/ weekly/ monthly basis against applicable limits. Limit breaches are reported to senior management and the Finance Committee.

Portfolio level Monitoring

Monitoring of the credit risk development at portfolio level is carried out regularly by Risk Management Department which is responsible for analysing and reporting the development to the Risk Management Committee, ALCO, and the Board of Directors. The reporting includes, among others, an analysis of the aggregate credit risk exposure, credit risk concentrations, changes in the risk profile, exposure against portfolio risk limits.

Management Information System (MIS)

Bank's Management Information System must provide reports for monitoring the condition of individual credits, and loan portfolio, including determining the adequacy of provisions and reserves.

Bank must have information systems and analytical techniques that enable management to measure the credit risk inherent in all on- and off-balance sheet activities. Bank must have in place a system for monitoring the overall composition and quality of the credit portfolio.

The Management Information System should provide:

- adequate and timely information on the composition of the credit portfolio and
- identification of any concentrations of risk.

Bank should also be able to analyse credit risk at the product and portfolio level to identify any sensitivities or concentrations.

An effective monitoring system shall ensure that the branch level functionaries and credit monitoring department in HO:

- i. Understand the current financial condition of the borrower
- ii. Monitor compliance with the existing terms and conditions
- iii. Assess the collateral in relation to the borrower's current condition, and

- iv. Identify non-performing accounts and enforces proper classification and loan loss provisioning.

Internal Controls and Audit

- a) The bank shall have an independent internal system for assessment of the credit risk management process to assist the board to review its effectiveness.
- b) A review of the lending process shall include analysis of the Loan Policy of the bank and actual performance of all functionaries involved in the credit function. It shall also cover origination, appraisal, sanction, disbursement, monitoring, collection, and handling procedures for the various credit functions provided by the bank.
- c) Internal audit reviews, through a designated Committee, shall assess compliance with the institution's credit policies and procedures.

This will require confirming the following:

- i. The credit granting function is carried out effectively,
 - ii. The credit exposures are within the prudential and internal limits set by the Board of Directors,
 - iii. Identification of areas of weaknesses in the credit risk management process, and
 - iv. Exceptions to the policies, procedures, and limits.
- d) Such internal reviews shall be conducted periodically and ideally once a year.

Credit Risk Mitigation

Banks/Lenders mitigate credit risk by using several methods.

- a) In controlling credit risk, the bank can use a variety of mitigating techniques which include collateral, guarantees and netting off loans against deposits (exercising right of set-off) of the same counterparty. While the use of these techniques will reduce or transfer credit risk, other risks may arise which include legal, operational, liquidity and market risks.
- b) Therefore, the bank should have comprehensive procedures and processes to control these risks and have them well documented in the policies.

Collateral Security

Security held by the institution to mitigate against credit risk should satisfy the following conditions:

- i. Regular monitoring of all collateralised transactions
- ii. All documentation used for lending against collateral securities must be binding to all parties and be legally enforceable
- iii. Necessary steps must be taken for obtaining and maintaining an enforceable security, for example registration, right of set-off or transfer of title must meet all the legal requirements
- iv. Procedures for timely possession and liquidation of collateral (in the event of default) as per SARFAESI Act should be in place
- v. Periodic valuations (once in three years) of the collateral should be undertaken to confirm that its value is adequate, and it remains realisable, and
- vi. Guidelines on various acceptable forms of collateral should be documented.

Other methods employed by banks to mitigate credit risk are:

a) Risk-based pricing: Risk based pricing of the loan is important for the bank to earn profits for reasonable return on capital. Loans and guarantees are priced to cover the

Bank's cost of funds, administration costs, the cost of the risk involved in the transaction and the cost of capital employed.

Bank, generally, charges a higher interest rate to borrowers who are more likely to default, by considering factors relating to the loan such as loan purpose, credit rating and loan-to-value ratio (LTV) and estimate the effect on yield (credit spread).

b) Covenants: Incorporating certain special stipulations on the borrower, who have lower ratings, into terms of sanction and loan agreements.

Credit Risk Scoring / Rating Framework

A Credit-risk Rating Module/ Framework is necessary to avoid the limitations associated with a simplistic and broad classification of loans/exposures into a "good" or a "bad" category.

Broadly, Credit Risk Rating System can be used for the following purposes:

- i. Individual credit selection, wherein either a borrower or a particular exposure/facility is rated as per the Credit Rating module/ Framework.

- ii. Pricing (credit spread) and specific features of the loan facility.
- iii. Portfolio-level analysis.
- iv. Surveillance, monitoring and internal MIS.
- v. Assessing the aggregate risk profile of bank. These would be relevant for portfolio- level analysis.

Bank should utilise the internal risk rating system in managing credit risk. The credit risk rating system should be consistent with the nature and size of loan.

Large Credit limits (Rs.25 lakhs and above) decisions may be based on credit risk ratings with an equal emphasis on qualitative elements such as the competence of management, experience, etc. After analysis, structuring, and pricing are completed, the loan proposal should be considered for sanction.

Credit Audit

The following needs to be in place for credit audit:

Compliance with pre-sanction and post-sanction processes set by the external and internal audit committee and compliance requirement by the credit risk management committee of the Board of Directors of the bank.

Bank credit audit could include:

- i. Quality of credit portfolio
- ii. Review of loan process
- iii. Compliance status of large value loans (above Rs. 25 lakhs)
- iv. Report on regulatory compliance
- v. Identification of loan distress signals
- vi. Review of loan restructuring decisions in terms of distress loans
- vii. Review of credit quality
- viii. Review of credit administration
- ix. Review of employees' credit skills especially at branch level

Credit audit may be conducted once in a year after the finalisation of the annual accounts of the bank and a report of findings to be placed to the Audit Committee of the Board.

Credit audit of large value loans (above Rs. 25 lakhs)

In case of large value loans, following are the action points for credit audit (review) of the

account:

- i. Verify compliance of bank's laid down policies and regulatory compliance with regard to sanction.
- ii. Examine adequacy of documentation.
- iii. Conduct the credit risk assessment.
- iv. Examine the conduct of account and follow up looked at by branch/ RO.
- v. Oversee action taken by branch/ RO in respect of serious irregularities.
- vi. Detect early warning signals and suggest remedial measures thereof.

Frequency of such credit audit of individual accounts may be fixed depending on the risk rating of the account.

4.5 Adequate Levels of Provisioning

The credit policy must clearly outline the provisioning procedures for all credit facilities and the capital charge to be held.

The spread of the portfolio credit-risk and the trends in credit migration would help the bank to determine the level of provisioning required to absorb unanticipated erosions in the credit quality of exposures.

In most cases, provisions for expected loan losses are based on the prevailing regulatory, statutory, and accounting directives. However, the management may consider a certain prudent level of “over-provisioning” facilitated by factors like the volume and the spread of credit-exposures in the “average” and “below average but acceptable” risk-rating categories or SMA-1 and SMA-2 categories.

Asset Quality evaluation

The asset portfolio in its entirety should be evaluated and should include an assessment of both funded and off-balance sheet items. The quality of the loan portfolio will be reflected in the non-performing assets and provisioning ratios, whilst exposure to the capital market and sensitive sectors will be indicated by the high volatility, affecting both valuations and earnings.

The key ratios to be analyzed are Non-performing Loans/Gross Loans ratio, Provisions/Gross Loans ratio and Provisions/Non-Performing Loans ratio.

Some issues which should be taken cognizance of, and which require further critical examination are:

- a. where exposure to a particular sector is above 10% of total assets,
- b. where non-performing advances which are not provided for are above 5% of the loan assets,
- c. where loan loss provision is less than 50% of the Gross NPA,
- d. rapid rates of loan growth. These can be a precursor to reducing asset quality as periods of rapid expansion are often followed by slowdowns which make the bank vulnerable,
- e. net impact of mark-to-market values of treasury transactions,
- f. correlation between the off-balance sheet items to the total assets.

Investments should be reflected on mark-to market basis and sticky investments should be treated as "non-performing".

Managing Credit Risk in Inter-bank Exposure

During its business, the bank may assume exposures on other banks, arising from trade transactions, money placements for liquidity management purposes, hedging, trading, and transactional banking services such as clearing and custody, etc. Such transactions entail a credit risk. Therefore, it is important that a proper credit evaluation of the banks is undertaken especially in case of money placement with other banks. Bank-wise exposure limits should be set considering the counter party and country risks. The credit risk management of exposure to banks should be centralized on a bank-wide basis.

The bank may evaluate the key financial parameters of the bank, such as:

- a) Capital Adequacy
- b) Asset Quality
- c) Liquidity
- d) Profitability

Credit risk assessment and mitigation

For credit risk assessment bank may adopt any of the following three approaches:

- development of statistical models through analysis of historical data,

- distribution of the firm's asset-value over a period of time (This model is based on the expected default frequency (EDF) model) and
- portfolio risk model.

The bank may follow any of these models and it should achieve the following:

- i. All credit exposure of the bank should be rated i.e., transaction – based and borrower based.
- ii. Identify concentration in the portfolios.
- iii. Identify problem credits before they become NPAs.
- iv. Identify adequacy/ inadequacy of loan provisions.
- v. Help in pricing of credit.
- vi. Determine the impact on profitability of transactions and relationship.

The bank shall undertake risk assessment based on the inputs from the following sources:

- I. Internal inspection (audit) reports and compliance reports.
- II. Reports of Concurrent Auditors
- III. Reports of Statutory Auditors.
- IV. Latest inspection report of NABARD
- V. Any changes in loan policy or change in focus/ priority areas
- VI. Significant change in key personnel in branches and administrative offices.
- VII. Sectorial trends and other environmental factors.
- VIII. Volume of business and risk prone credit.
- IX. Substantial variations in performance vis-à-vis budget in terms of business and profitability.

Off-balance sheet Exposures (Contingent Liabilities)

Risk Identification and Assessment of Limits

Credit Risk in non-fund based business of banks need to be assessed in a manner similar to the assessment of fund based business since it has the potential to become a funded liability in case the customer is not able to meet his commitments. Financial guarantees are generally long term in nature, and assessment of these requirements should be similar to the evaluation of requests for term loans. As contracts are generally for a term of 2-3 years, banks must obtain cash flows over this time horizon, arising from the specific contract they intend to support, and determine the viability of financing the contract.

Risk Monitoring and Control

For reducing credit risk on account of such off balance sheet exposures, banks may adopt the following measures:

- i) Banks must ensure that the security, which is available to the fund based credit facilities, also covers the LC and the guarantee facilities. It will be appropriate to take a charge over the fixed assets as well, especially in the case of long-term guarantees.
- ii) In the case of guarantees covering contracts, banks must ensure that the clients have the requisite technical skills and experience to execute the contracts. The value of the contracts must be determined on a case-by-case basis, and separate limits should be set up for each contract. The progress vis-à-vis physical and financial indicators should be monitored regularly, and any slippages should be highlighted in the credit review.
- iii) The strategy to sanction non-fund facilities with a view to increase earnings should be balanced vis-à-vis the risk involved and extended only after a thorough assessment of credit risk is undertaken.

Roles and Responsibility of Board of Directors & Senior Management

Board of Directors

The board of directors shall be ultimately responsible for providing overall strategic direction to the Bank through approving and reviewing the credit risk management policy.

The board shall ensure that:

- (i).An appropriate committee (Risk Management Committee) is in place to oversee the credit risk management.
- (ii).The Credit Risk Management (as part of Risk Management Policy) and Credit Policy are reviewed, approved, and effectively communicated throughout the institution.
- (iii).There is an internal audit function capable of assessing compliance with the credit policies and management of the entire credit portfolio,
- (iv).The delegation of authority and approval levels of credits are clearly defined, and
- (v).Management provides reliable and appropriate reports on loans, provisioning and write-offs on credit loan losses and audit findings on the credit granting and monitoring processes with sufficient frequency.

Senior Management

Management shall implement the credit strategy and policies approved by the board of directors and develop procedures for effective management of credit risk.

Management shall ensure that:

- i) The credit granting functions conform to the laid down systems and procedures,
- ii) written policies and procedures are developed, implemented and responsibilities of the various functions are clearly defined,
- iii) The credit policies are communicated throughout the institution, implemented, monitored, and reviewed periodically to address any changes,
- iv) Compliance with internal exposure limits, prudential limits and regulatory requirements is enforced,
- v) The development and implementation of appropriate reporting systems with respect to the content, format and frequency of information concerning the credit portfolio,
- vi) Internal audit reviews of the credit risk management system and credit portfolio are undertaken regularly, and
- vii) Adequate research is undertaken for any new products or activities to ensure risks are appropriately identified and managed. These products must receive prior board approval.

Conclusion

The risk management is a complex and tedious process. The bank must follow the RBI's and NABARD's guidelines. There are benefits from having risk management system in place, which can help control the menace of rising NPAs.

Liquidity Risk

1. Introduction

Liquidity risk is defined as the risk to bank's earnings or capital arising from its inability to meet its obligations as they fall due, without incurring significant costs or unacceptable losses.

It also arises from the Bank's failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly with minimal loss in value.

Impact of liquidity risk could be in the form of penalties, loss of funds, loss of business and reputational damage due to the bank's inability to meet the funding requirements of its customers.

Liquidity risk management systems involve analysing Bank's on and off-balance sheet positions to forecast future cash flows but also how the funding requirements could be met.

The main objectives of liquidity risk management processes and strategies are:

- To ensure that bank's balance sheet earns a desired net interest margin (NIM), without exposing the bank to undue risks due to interest rate volatility.
- To plan and structure a balance sheet with a proper mix of assets and liabilities, to optimize the risk/return profile of the bank
- To appraise its ability to meet its cash flow and collateral needs (under both normal and stressed conditions) without having a negative impact on day-to-day operations or its overall financial position.

To mitigate that risk by developing strategies and taking appropriate actions designed to ensure that necessary funds and collateral are available when needed.

2. Identification of Liquidity Risk

The bank should define and identify the liquidity risk to which it is exposed for each major on and off-balance sheet position, and other contingent exposures that may affect the bank's sources and uses of funds and for all currencies in which the bank is active.

3. Measuring and Managing Liquidity Risk

Measuring and managing liquidity needs are vital for effective operation of the bank. The bank should measure not only liquidity position on an on-going basis but also examine how liquidity requirements are likely to evolve under different assumptions or scenarios.

Liquidity measurement involves assessing the bank's cash inflows against its outflows to identify the potential for future net funding shortfalls. An effective liquidity risk measurement and monitoring system in place, helps in managing liquidity in times of crisis and also optimize return through efficient utilization of available funds. Key elements of an effective risk management process include an efficient Management Information System (MIS), systems to measure, monitor and control risks.

4. Measurement of liquidity position

The bank must establish appropriate internal guidelines on the level of different ratios and ensure prompt corrective actions are undertaken to address any liquidity shortfall.

5. Minimum Liquidity Ratio

Currently banks are required to maintain a minimum of 18.00 % (from 05 April, 2024) as Statutory Liquidity Ratio, and 4.50% as Cash Reserve Ratio of their total net demand and time liabilities as on the last Friday of the second preceding fortnight, valued in accordance with the method of valuation specified by the Reserve Bank of India from time to time, in liquid assets. The bank can however develop its own higher minimum liquidity ratio based on its own risk appetite.

6. Loan to Deposit Ratio

Bank should compute at month end, a loan to deposit ratio. Such ratio provides a simplified indication of the extent to which the bank is funding illiquid assets by stable liabilities. The bank may set a trigger loan-deposit ratio above which liquidity risk management should be enhanced.

7. Maturity Profile

Analysing funding requirements involves the construction of a maturity profile. A cash flow projection estimates the bank's inflows and outflows and thus establishes net deficit or surplus (GAP) over different time bands/ buckets.

The focus of the bank should be on short term mismatch i.e. 1-14, and 15-28 days' time band. The mismatches (negative gap between cash inflows and outflows) during 1-14, and 15-28 days' time band in normal course should not exceed a certain percentage (say 20%) of the cash outflows in each time band. The ceiling for the other time buckets must

be fixed by ALCO.

Bank should review the assumptions utilized in managing liquidity frequently to determine that it continues to be valid, since the bank's future liquidity position will be affected by factors that cannot always be forecast with precision given the rapidity of change in financial markets.

The ALCO will prepare cash flow analysis i.e. outgoing commitments compared with inflow of funds, in different time maturity bands/ buckets, identifying net position or mismatches, etc. and will take necessary measures to overcome liquidity risk.

8. Liquidity Risk Monitoring

A monitoring system shall consist of limits, guidelines and trend development that will enable the management to monitor compliance with approved risk limits/tolerance and track variances.

9. Key Liquidity Factors

The following key liquidity factors should be monitored closely:

- Seasonal pattern of accretion of deposits and disbursement of loans
- The maturity profile of cash flows under varying scenarios
- Potential liquidity needs for meeting new loan demands, availment of unavailed credit limits, devolvement of contingent liabilities (letters of credit and bank guarantees), potential deposit losses, investment obligations, statutory obligations, etc.
- Economic and money market trends
- Monitoring flow of high value deposits say, of Rs. 1.00 crore and above, to track the volatile liabilities
- Tracking the impact of prepayments of loans, premature closure of deposits
- Analyzing the behavioral maturity profile of various components of on/off-balance sheet items on the basis of assumptions and trend analysis.

10. Liquidity Management Tools

- **Funding strategy:** The bank shall focus on CASA deposits, term deposits from large number of small depositors thereby reducing dependency on few large depositors; minimize ALM mismatch position, etc.
- **Funds deployment strategy:** The bank shall deploy the raised funds in various instruments, subject to overall guidelines issued by NABARD in permitted markets with focus on liquidity, marketability, and optimum yield.
- **Contingency plan:** The bank will build up contingency plans leading to most effective funding strategy depending upon the timing, urgency, duration for which funds are required, availability of funds, seasonality etc. on an ongoing basis.
- **Internal control:** The bank shall have an adequate system of internal controls over its liquidity risk management process.
- **Asset Liability Committee (ALCO):** ALCO is responsible for ensuring that the bank's operations lie within the parameters set by RBI/ NABARD and by its Board of Directors.

11. Roles and Responsibility of Board of Directors & Senior Management

The prerequisites of an effective liquidity risk management include an informed board, capable management, staff with relevant expertise and efficient systems and procedures. It is the responsibility of the bank's board and management to ensure that the bank has sufficient liquidity to meet its obligations as and when they fall due.

a). Board of Directors

The board shall:

- Approve and review significant policies that govern bank's liquidity risk
- Establish an appropriate structure for the management of liquidity risk and identify lines of authority and responsibility for managing liquidity risk exposures
- Take appropriate steps to ensure that liquidity risk is adequately identified, measured, monitored and controlled, and
- Monitor the bank's overall current and prospective liquidity risk profile on a regular basis

- Review adequacy of the contingency plans of the bank

b). Senior Management

The bank shall have an appropriate management structure to oversee the day to day and long term management of liquidity risk in line with the approved strategy, policies, and procedures. The senior management shall:

- Periodically review risk taking limits,
- Implement management information systems and standards for measuring liquidityrisk,
- Convert board's approved strategies and policies and risk tolerances into operational standards, and
- Immediately communicate any material changes in bank's current or prospective liquidity position to the board.

Introduction

Traditionally, credit risk management was the primary challenge for the banks. With progressive deregulation of interest rates and foreign exchange, market risk arising from adverse changes and fluctuations in market variables, such as interest rate, foreign exchange rate, credit spreads, equity price and commodity price, has become relatively more important. Even a small change in market variables causes substantial changes in income and economic value of banks.

Market risk is the risk of loss resulting from changes in the value of assets and liabilities (including off-balance sheet assets and liabilities) due to fluctuations in risk factors such as interest rates, foreign exchange rates and stock prices and the risk of loss resulting from changes in earnings generated from assets and liabilities. Market Risk can also be defined as the risk to the bank's earnings and capital due to changes in the market level of interest rates or prices of securities, foreign exchange, and equities, as well as the volatilities of those prices.

The bank places the safety and security of investments ahead of the potential for return, as such it is only willing to take on a low level of exposure to market risk.

Market risk takes the form of:

1. Interest Rate Risk
2. Foreign Exchange Risk
3. Equity Price Risk
4. Commodity Risk

1. Interest Rate Risk

Changes in interest rates affect the bank's earnings by changing its net interest income and the level of other interest sensitive income and operating expenses.

Changes in interest rates thus can have adverse effects both on the bank's earnings, and its capital.

Interest rate risk is the risk where changes in market interest rates might adversely affect a bank's financial condition. The regulatory restrictions in the past had greatly reduced many of the risks in the banking system. Deregulation of interest rates has, however, exposed the banks to the adverse impacts of interest rate risk. The Net Interest Income (NII) or Net Interest Margin (NIM) of banks is dependent on the movements of interest

rates. Any mismatches in the cash flows (fixed assets or liabilities) or repricing dates (floating assets or liabilities), expose banks' NII or NIM to variations. The earning of interest on loans and advances, and the interest cost on deposits are now closely related to market interest rate volatility. The Bank measures its net interest income risk by estimating the sensitivity of the accumulated net interest income during the next twelve months to changes in the level of interest rates.

a) Interest Rate Identification and Risk Measurement

An asset or liability is normally classified as rate sensitive if

- Within the time interval under consideration, there is a cash in -flow for instance, repayment of installments of term loans etc.
- The interest rate resets/reprices contractually during the interval. For instance, changes made in the interest on CC accounts, term loan accounts during the repayment period (before maturity).
- Changes in the administered interest rates by the Reserve Bank of India

The risk from earning perspective can be measured as changes in the Net Interest Income. The traditional gap analysis will be considered as a suitable method to measure the interest rate risk for the bank. The risk gap will be measured by calculating gaps over different time intervals as at a given date (usually one year). It will monitor the mismatches between rate sensitive liabilities and rate sensitive assets (including off-balance sheet positions) by preparing the gap report. The bank should have a forecast regarding the interest rates in the market and accordingly fix up gap limits for various time buckets. The ALCO may be authorized for the same.

b) Risk/Exposure Limits for Investments

The risk/exposure limits for Investments shall be as per the Investment policy of the Bank. All deviations shall be reported to the Risk Management Committee of the Bank.

c) Interest rate risk in Trading Book

Currently, the bank is not doing any trading in the securities. Therefore, the modified duration analysis, earnings at risk analysis for measuring and monitoring of interest rate risk will be taken up in due course.

d) Management of Interest Rate Risk

The management of Interest Rate Risk should be one of the critical components of

market risk management in bank.

The Bank's strategy is to obtain cost-efficient funding, CASA deposits as well as low cost deposits, refinance, from diversified sources and provide lending that is tailored to the needs of its customers

e) Reporting

While ALCO will have track on liquidity and interest rate on an on-going basis, the Risk Management Committee shall be kept informed about the deviations and review the liquidity position of the bank in all meetings of the Risk Management Committee.

f) Roles and Responsibility of Board of Directors & Senior Management

i. Board of Directors

The responsibilities of the board of directors include the following:

- reviewing the overall objectives of the bank with respect to interest rate risk and ensuring that management takes the steps necessary to identify, measure, monitor and control these risks,
- review periodically, at least once a year, the interest rate risk management policy,
- to annually review and approve maximum limits for exposure to market risk,
- approving policies that identify lines of authority and responsibility for managing interest rate risk.

ii. Senior Management

The senior management has the responsibility of implementing all approved policies that govern Market Risk and developing procedures for effective management of the market risks.

It is the responsibility of senior management to maintain:

- Appropriate limits on risk taking
- Adequate management information systems (MIS) and standards for measuring interest rate risk are in place
- A comprehensive interest rate risk reporting and management review process, and effective internal controls are there.

To fulfil the above responsibilities, management shall periodically review the bank's interest rate risk management policies and procedures to ensure that they remain

appropriate and sound. It shall also periodically update the board of directors regarding interest rate risk measurement, reporting and management procedures.

2. Foreign Exchange Risk

Foreign exchange risk is the current or prospective risk to earnings and capital arising from adverse movements in currency exchange rates. The potential for loss arises from the process of revaluing foreign currency positions on both on- and off- balance sheet items. Changes in the exchange rate of currencies can lead to a loss in the value of investments denominated in foreign currencies.

Presently, the bank is mainly confined to domestic operations.

1. Equity Price Risk

If the price of equities listed and traded on the major stock exchanges changes, then the bank's balance sheet may be affected by a fall in the value of its equities or bonds. This is not applicable to the bank.

2. Commodity Risk

Since bank is not dealing in commodities, this is not applicable to the bank.

Non - Financial Risks

- ❖ **Operational Risk**
- ❖ **Compliance Risk**
- ❖ **IT Risk**

Operational Risk Management

1. Introduction

Growing number of high-profile operational loss events worldwide have led the banks to increasingly view operational risk management as an integral part of the risk management activity. Management of specific operational risks is not a new practice, it has always been important for the banks to prevent frauds, maintain the integrity of internal controls, reduce errors in transaction processing, etc. Unlike market and credit risk, which tend to be in specific areas of business, operational risk is inherent in all business processes.

The Bank's operational risk management focuses on proactive measures in order to ensure business continuity as well as the accuracy of information used internally and reported externally, a competent and well-informed staff, and its compliance with RBI/NABARD regulations and guidelines and internal policies as well as on security arrangements to protect the physical and ICT infrastructure of the Bank.

2. Operational Risk Defined

The common industry definition as defined in the RBI guidelines and the Basel II Accord for Operational Risk is–

“as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.”

Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

This definition is based on the underlying causes of operational risk. It seeks to identify why a loss happened and at the broadest level it includes mainly four causes:

- people,
- processes,
- systems and
- external factors.

3. Operational Risk Loss

An Operational Risk Loss is defined as loss from inadequate or failed internal processes, people and/or systems, or from external events causing any of the following adverse impact:

- Events constituting actual loss.
- Events with future impact.
- Events without loss (or accidental gain)
- Events which seriously jeopardize the business operations (example: System downtime, strike etc.)
- Events caused / causing threat to employee life

4. Objectives of Operational Risk Management Policy

The main objectives of Operational Risk Management Policy are:

- To meet Basel-II requirements on Operational Risk Management
- To identify and introduce operational risk management function across the entire bank, so as to assess exposure with respect to Operational Risks and take appropriate actions
- To establish a management structure with clear lines of responsibility, accountability and reporting with respect to operational risk
- To strengthen the internal control environment reducing the probability and potential impact of Operational Risk losses

5. Categories (risk events) of Operational Risk Relevant to the Bank

Seven categories of Operational risk (risk events) having the potential to result in substantial losses to the bank includes:

- 1. Internal fraud:** Losses due to intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
- 2. External fraud:** Losses due to robbery, forgery, cheque kiting, misrepresenting information to obtain financial benefits/ loans, and damage from hacking of computer.
- 3. Employment practices and workplace safety:** Losses arising from

workers compensation claims, violation of employee health and safety rules, discrimination claims, and general liability.

4. Clients, products, and business practices: Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product. For example, fiduciary breaches, misuse of confidential customer information, money laundering, and sale of unauthorized products and/ or mis- selling various products.

5. Damage to physical assets: Losses arising from loss or damage to physical assets from a natural disaster or other events. For example, terrorism, vandalism, earthquakes, fire, and floods.

6. Business disruption and system failures: Losses arising from disruption of business or system failures. For example, hardware and software failures, telecommunication problems, and utility outages.

7. Execution, delivery, and process management: Losses from failed transaction processing or process management, from relations with trade counterparties and vendors. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, and vendor disputes.

6. Main Factors/Causes Generating Operational Risk

The events mentioned above may occur due to both, internal and external factors in the following areas:

1. Internal factors

- i. People (Employees):** The risk occurring from the deliberate or unintentional actions or treatment of employees and/or management. Bank can achieve significant improvements in its control of operational risk and reduce exposure if it creates an appropriate risk culture, in which employees are aware of operational risks and are encouraged to learn from their mistakes.
- ii. Processes and systems:** Bank's operations are supported by different systems and processes, such as IT systems, human resource management systems, credit, market, insurance, liquidity risk management, hardware, software,

communications, and their interfaces.

2. External factors

External events can have a major impact on the bank. The expected and unexpected changes to its operations can be major sources of operational risk. The Bank should have in place appropriate arrangements, having regard to the nature, scale, and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness.

- i. Disruptive events include fire, flooding, earthquakes, terrorist actions, vandalism, power failures, etc. The Bank should assess the potential risk for such events to happen, design and put in place disaster recovery systems and procedures, with a view to ensuring continuity of activity. Against the monetary loss derived from such events the Bank should evaluate potential cost and acquire proper insurance.
- ii. Use of Consultants and Outsourcing of Services Outsourcing arrangements require careful management to drive benefits, and where they are not managed adequately the degree of operational risk faced by the Bank may increase. The excessive use and dependency on consultants can be reduced for activities that may be more effectively developed internally.

7. Operational Risk Management Process

Operational Risk Management consists of sequence of activities and decisions involved to manage operational risk. The key elements in Operational Risk Management process would include:

- Risk identification – Identification of Operational Risks across various products and processes of the Bank
- Risk Assessment – Assessing the potential likelihood and impact caused by Operational Risk events and the quality of the control environment.
- Risk Categorization – Common language for risk / loss classification
- Risk Monitoring-Monitoring unacceptable changes in the risk profile over a period of time.
- Risk Mitigation – Various measures adopted by the Bank to mitigate / manage

key Operational Risks and tracking of mitigation mechanism put in place so that the risk levels stay within acceptable tolerance levels.

- Risk Reporting – Providing a snapshot of key operational risks and the internal control environment.
- Performance Management – Aligning reward structure to management of risks subsequent development of feasible operational risk measurement, monitoring and control.

8. Identification and Risk Assessment

- The bank must identify and assess the operational risk inherent in all material products, activities, processes, and systems.
- It should also ensure that before new products, activities, processes, and systems are introduced or undertaken, the operational risk inherent in them is identified clearly and subjected to adequate assessment procedures.
- The bank must consider both internal factors such as,
 - nature of bank's activities, organizational changes, quality of personnel, employee turnover and the complexity of computer systems and processes, etc.

and external factors such as

- economic conditions, fraud, robbery, changes in industry and technological advances etc. that could adversely affect the achievement of the bank's objectives.

Other external risks also to be considered include

- natural disaster (earthquake, flood, etc.), fire and power breakdown, terrorism, security breaches, database corruption, virus and malware attacks and system configuration failure.

In identifying and assessing operational risk, the bank shall:

Collect and analyse loss data: Internal operational loss data provide meaningful information for the assessment of bank's exposure to operational risk and the effectiveness of its internal controls. The bank will build up a loss database of the bank as one of the operational risk management measures.

In addition, bank shall use all or some of the following tools as the case may be:

- **Audit findings:** While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors
- **Self - Risk-Assessment:** The bank shall assess its operations and activities through a menu of operational risk events.

The bank can use one or more of the following tools to evaluate Self or Risk-Assessments:

- workshops in which various business units assess their risk exposures,
- checklists on which managers are asked to fill in questionnaires that identify the levels of risk and the related controls.

9. Key Risk Indicators: Risk indicators are statistics or metrics, often financial, which can provide insight into bank's financial position. These indicators should be reviewed periodically (often monthly or quarterly) to alert the bank regarding changes that may be indicative of risk concerns. Examples of such indicators are the number of failed trades, staff turnover rates and frequency of errors and omissions.

10. Risk taking ability or appetite

Risk appetite is a function of risk taking ability of the bank. The bank will decide the level of appetite by estimating its capacity to manage the risk taken and the possible impact if the risk were to turn true.

The table below details the risk appetite of the bank under the broad categories of risk. The risk appetite under each category will be reviewed and revised by the board following material changes to the internal or external environment of the bank.

11. Broad Categories of Risk Events and Acceptable Level of Risk Appetite in Bank

Operational Risk Category (Risk Event)	Risk Appetite	Details
<i>a. Internal and external fraud</i>	Zero risk appetite	Due to potential for significant financial loss and reputational damage, the bank will not accept any exposure to risk in this area. Bank will therefore have good systems and procedures internal control systems to avoid and manage fraud proactively.
<i>b. Clients, products and business practices</i>	Zero risk appetite	Due to potential damage to the reputation, the bank will not take on any exposure to risk in this area. Bank will have strict systems and procedures which will ensure that KYC is implemented correctly, and that Money Laundering is avoided.
<i>c. Employment practices and workplace safety</i>	Low risk appetite	As the bank employs officers and other staff, it cannot avoid some degree of exposure in this risk area. HR policies will be designed to reduce the risk as much as possible. Imparting training to all employees will also help to reduce the risk as much as possible.
<i>d. Damage to physical assets</i>	Low risk appetite	The assets required to operate the business are subject to damage, the bank cannot avoid accepting a low level of Exposure to risk in this area. Insurance of assets will be one of the primary means of managing risk. The Administration will effectively supervise the assets. Proper record on maintenance of all assets will be done to avoid this risk.
<i>e. IT systems and software failures</i>	Low risk appetite	Due to its larger dependence on the IT infrastructure for the continued operation of the business, the bank will only accept a low level of risk in this area.
<i>f. Execution, delivery, and process management</i>	Moderate risk appetite	The board is willing to accept exposure to a moderate level of risk in this area. The processes will however be reviewed frequently to keep it up to date and effective.

12. Risk Measurement

The tracking of individual risk incident data is an essential pre-requisite to the development and functioning of a robust operational risk management measurement system. For this purpose

1. Bank shall constitute a structured process for reporting operational risk incidents on a regular basis.
2. Each business unit must ensure that the operational risk incident data is submitted to the risk management department (collecting and processing data collected from various sources and reporting the same) and that the required data meets all established standards for timeliness and integrity.
3. A 'root cause and lessons learnt' analysis can be drafted for each risk incident by the reporting unit. Risk Management Committee centrally would compile all the 'lessons learnt' analysis and ensure that the same is circulated on a periodic interval.
4. Risk Management Department would circulate these incidents/reports to all levels in the bank, including all branches.

13. Risk Monitoring

Based on the Risk or Self Assessments and other risk analyses, the Risk Management Committee in close coordination with various departments (Functional / Support/ Regional Offices) would identify and monitor Key Risk Indicators (KRI), reporting of which enables the management to monitor and mitigate risks that are exceeding acceptable levels.

Some of the Operational Risk limits (in KRI) which are proposed include the following:

Sr. No.	Item	Risk TRIGGER limit
1	Excess CRR	If actual CRR of the Bank exceeds <u>1</u> % over the Prescribed CRR limit
2	Cash retention limit	Aggregate cash holding level of branches exceeding the limit prescribed.
3	Non-working ATMs	5% of the total number of ATMs in the Bank

4	Pending reconciliations of ATM transactions	Reconciliations pending beyond one month
5	Incomplete KYC	KYC incomplete even in one of deposit + loan Accounts in operation
6	Penalties levied on the bank (at the branch) by the Income tax dept., Banks' Ombudsman, local authorities	Even if one penalty levied in any branch.

14. Risk Mitigation/Controls of operational risk

Several methods may be adopted for mitigating the operational risk:

1. Bank must have policies, processes, and procedures to control and/ or mitigate operational risks.
2. Bank should ensure that internal controls are in place as appropriate to address operational risk including:
 - Clearly established authorities and/ or processes for approval
 - Close monitoring of assigned risks limits.
 - Safeguard for access to, and use of, bank assets and records.
 - Appropriate staffing and training to maintain expertise.
 - Regular verification and reconciliation of transactions and accounts and so on.
3. Regarding fraud prevention, detection and investigation, bank must ensure following:
 - Strong KYC Policy and process
 - Training of staff on preventing and detecting frauds.
 - Root cause analysis of fraud events
 - Annual review on frauds
 - Exemplary punishment on intolerance to frauds
 - Regular security audits
 - Process specific fraud risk controls including maker & checker control.
Controlling fraud risks in - Phishing, skimming, hacking, identity theft, spam mail, virus.
 - Timely detection and reporting

- Strengthening and clearly spell out of internal control systems.
 - Compliance with the provisions of Income Tax and GST.
3. For managing human resource Risk in the Bank, the Bank shall ensure:
- Recruitment of qualified and skilled staff (including specialist officers for specialized functions such as IT, Law, Security, etc) on continuous basis without leaving any gaps.
 - Maintaining a healthy age profile combining young age group with skill competence and experience in the higher age group
 - Optimal deployment of human resources with the right person for the right job
4. Training and placement activities covering new staff and existing staff will include:
- Knowledge and skills relating to the area of risk management.
 - System of internal controls including effectively communicating significant changes to controls to all affected officers.
 - Risks in bank's products and processes along with transparent rules and regulations with updated manuals covering different areas of bank's working.
 - Job Rotation on regular basis
 - Succession planning
5. Losses that might arise from business disruptions due to telecommunication or electrical failures can be mitigated by establishing backup facilities.
6. Loss due to internal factors, like employee fraud or product flaws, which may be difficult to identify and insure against, must be mitigated through strong internal auditing procedures.
7. The bank should have a system for ensuring compliance with RBI/NABARD regulations and guidelines and internal policies.
8. New products or major changes in existing products must be introduced after all relevant risks are analysed and processed and controls established to manage those risks.
9. Bank must have a sound technology infrastructure (relating to the physical and logical structure of information technology and communication systems,

individual hardware and software components, data, and the operational environment) that meets current and long-term business requirements by:

- providing sufficient capacity for normal activity levels as well as peaks during periods of market stress,
- ensuring data and system integrity, security, and availability, and
- supporting integrated and comprehensive risk management.

10. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service provider and the bank.

11. Losses that might arise on account of natural disasters can be insured against. It should periodically review its disaster recovery and business continuity plans so that they are consistent with the bank's current operations and business strategies.

15. Risk Reporting

To reinforce Operational Risk culture and provide periodic updates to the Risk Management Committee and on the Operational Risk Profile of the Bank and various departments, Risk Management Committee would design a Risk Reporting framework listing the reporting requirements from various departments, its periodicity and responsibility. Chief Risk Officer/ Head of Risk Management Department shall be responsible for providing the data and information to the Risk Management Committee.

An illustrative example of reports that would be placed to the Risk Management Committee would be as follows:

- ▶ Reporting of Operational Risk Losses by departments/branches
- ▶ Trends of Losses by business line over a period of time.
- ▶ Key Operational Risks by departments/branches
- ▶ Summary of Self or Risk Assessment results for various department, overall residual risk and aggregate Risk Profile of the department/branches
- ▶ Key control improvement opportunities, progress and implementation plan

- ▶ KRIs for various departments/branches including their trends over a period of time.

16. Roles and Responsibility of Board of Directors & Senior

Management

a). Board of Directors

- Define the operational risk strategy and ensure that the strategy is aligned with theco-operative's overall business objectives.
- Approve and periodically review the Operational Risk Management framework andOperational Risk Policy developed by the management of the bank.
- Approve the Bank wide risk tolerance and review the Bank's exposure to its key Operational Risk.
- The Board of Directors shall review, at least annually, the appropriateness of thelimits and the overall operational risk appetite and tolerance.
- Assess the effectiveness of risk mitigation plan implemented by the Bank to manageOperational Risk.
- Provide strategic guidance on various initiatives undertaken by the Bank towardsmanagement and mitigation of Operational Risk.
- Establish a management structure with clear lines of responsibilities, accountability,and reporting.
- Ensure compliance with regulatory disclosure requirements on operational risk.

b). Senior Management

Senior management shall be responsible for implementing the operational risk management framework approved by the Board of Directors.

- To translate operational risk management framework established by the Board ofDirectors into specific policies, processes, and procedures.
- To clearly assign authority, responsibility, and reporting relationships to encourage accountability.
- To ensure that the necessary resources are available to manage operational risk

effectively.

- To ensure that bank's activities are conducted by competent staff with necessary experience and technical capabilities.
- Ensure that policies have been clearly communicated to staff at all levels.
- Pay particular attention to the quality of documentation controls and to transaction-handling practices.
- To ensure that the bank's HR policies are consistent with its appetite for risk and are not aligned to rewarding staff that deviate from the policies.

c). Audit and Inspection Department

- Provide assurance on the reporting quality of data on Key Risk Indicators, Self or Risk Assessment and Loss data reported by various reporting departments as well as on the quality of operational risk management in the bank.
- Share audit findings and observations with Risk Management Committee as a background for facilitating risk assessments.
- Report to senior management, Risk Management Committee and Audit Committee the results of their independent reviews of the operational risk management processes both at the level of corporate office and branches.

d). Compliance Function

- The Chief Compliance Officer or Officer in - charge looking after Compliance functions of the Bank, shall be the member of the committee for operational risk management.
- The bank to ensure that compliance risk in new products and processes being introduced get identified and appropriate risks mitigates are put in place before launching the same.

e). Risk Management Committee (RMC)

- Risk Management Committee (RMC), will be primarily responsible for ensuring effective management of the Operational Risks in the Bank
- Review various Operational Risk related issues and incidents and focus on any important issues requiring attention at the policy or process level.

RISK MANAGEMENT POLICY

- Review the risk profile, understand future changes and threats, and prioritize action steps.
- Review and approve the development and implementation of Operational Risk methodologies and tools, including assessments, reporting, etc.,
- Monitor and oversee the implementation of the Operational Risk Management framework in the Bank.
- Review the results of root cause analysis of loss events and approve changes in the internal control mechanism.
- Approve Operational risk capital methodology.

1. Introduction

In July 2005 Reserve Bank of India (RBI) set up a working group with participation from banks to review the present system of compliance functions and recommend measures to strengthen it. Based on the recommendation of the group, in April 2007 RBI issued comprehensive guidelines on Compliance and Compliance Functions in Banks. Banks were directed to put in place a robust compliance system for strict observance of all statutory provisions contained in various legislations such as Banking Regulation Act, Reserve Bank of India Act, Foreign Exchange Management Act, Prevention of Money Laundering Act etc. as well as to ensure observance of other regulatory guidelines issued from time to time, standards and codes prescribed by BCSBI, IBA, FEDAI, FIMMDA etc., and also each bank's internal policies and fair practices code.

Non-compliance of statutory provisions, regulatory guidelines and internal policies can give rise to various risks including legal problems, material financial loss, loss of reputation and regulatory sanctions.

Compliance functions are one of the key elements in the Bank's Corporate Governance Structure, which must be adequately enabled and made sufficiently independent so that it is capable of identifying, evaluating & addressing Legal and Reputation Risks.

"The Basel Committee on Banking Supervision (BCBS) paper defines Compliance risk as "the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities".

Banking compliance can be broadly segregated in three parts

- a) Internal compliance
- b) Regulatory Compliance
- c) Legal Compliance

The internal compliance means adherence to the internal policies formulated by the bank's Board. Thus, internal compliance would be applicable to all employees of the bank.

The regulatory and legal compliance, on the other hand, is applicable to the bank as a whole. The Bank itself would be responsible for ensuring adherence to the extant

statutory and regulatory instructions and also, for abiding by the laws of the land, both in letter and spirit.

The compliance area is critically important in identifying, evaluating, and addressing legal and reputational risks.

2. Objective of Compliance Risk Management

The objective of the compliance function is to minimize the deviations, or in the event of occurrence, to ensure that there is a process to promptly respond to and redress the anomalies and to tighten the compliance regime in the Bank.

Other objectives of the Compliance Risk Management include:

- to establish pro-active compliance management culture, which includes measures to identify, monitor and control compliance risk inherent in various business lines and activities of the bank,
- to develop a comprehensive database on various compliance areas to monitor and improve compliance functions,
- to Improve confidence of all customers, counterparties, shareholders, investors, debt holders, regulators, government bodies and all other stake holders in operational and financial integrity.

3. Fall-out/ consequences of non-compliance

The consequences of certain non-compliances and non-fulfilment of compliance responsibilities could be critical for the bank such as:

- Legal Problems
- Imposition of penalties on the bank
- Regulatory sanctions and
- Loss of reputation for the bank

4. Risk Control

Risk Management Department at Head Office shall continue to play the central role in the area of identifying the level of compliance risk.

The Risk Management Department can provide vital inputs on possible breaches of

regulatory guidelines and appropriate risk mitigating checks and balances, if required:

- By screening of prospective products and services before they are launched, and
- By pointing out deficiencies in documentation.

5. Implementing Compliance Risk Management

In the process of implementing compliance risk management, the Bank will cover the following:

- At least once a year, identify and assess the main compliance risks facing the bank and formulate plans to manage them.
- Develop compliance program to identify, evaluate, and address legal and reputational risks.
- Focus of the Compliance Function on regulatory compliance, statutory compliance, compliance with fair practice codes and other codes prescribed / suggested by self- regulatory organizations, government policies, bank and internal policies and prevention of money laundering and funding of illegal activities.
- Compliance risks in all new products and processes shall be thoroughly analysed and appropriate risk mitigation put in place before launching new products, services and processes
- Training of staff and enhancing awareness on Compliance on ongoing basis
- To circulate the instances of compliance failures among staff along with preventive instructions
- Checklist on the compliance aspects may be made part of the inspection report for the inspectors / concurrent auditors to verify the level of compliance.
- In case of compliance failures staff accountability to be fixed and appropriate remedial or disciplinary action is to be taken
- Non-compliance with any regulatory guidelines and administrative actions initiated against the bank and or corrective steps taken to avoid recurrence of the

lapses shall be disclosed in the annual report of the bank.

- Ensure that the bank reports promptly to the Board of Directors, Risk Management Committee and Audit committee of Board on any material, compliance failure (e.g., failure that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation).

6. Disclosures

The bank will ensure that all mandated disclosures will be made within the time limit as mandated by the regulators – NABARD, RBI, and RCS. Illustratively the current mandated disclosures include:

- Balance sheet disclosures on various aspects including off balance sheet items
- Maintenance of CRR and SLR
- KYC compliances
- Recovery and remittance of TDS / service tax as applicable and filing of returns from time to time.
- Reporting of suspicious Transaction Report (STR) and Cash Transaction Report (CTR) to Financial Intelligence Unit (FIU)
- CRAR disclosures
- Penalties levied on the bank
- Complying with court orders failing which contempt of court could arise
- Complying with statutory and regulatory restrictions and ensuring no violation
- Complying with IRAC norms
- Adherence to the prudential norms for classification, valuation, operation of investment portfolio for cooperative banks as prescribed by RBI / NABARD

7. Structural Framework for Compliance Risk

The Broad framework for compliance risk would inter-alia include:

- Designating a senior officer as independent Compliance Officer
- Formulating a Compliance Policy for the Bank

- Monitoring compliance guidelines in consultation with the Audit Committee of the Board or any other Specific Board Committee constituted for the purpose by the Board

8.Roles and Responsibility of Board of Directors & Senior

Management

a). Board of Directors

The Board would be responsible for ensuring that

- An appropriate compliance policy is in place in the bank to manage compliance risk and shall be overseeing its implementation.
- Compliance issues are resolved effectively and expeditiously by Senior Management with the assistance of Compliance Officer.
- There is no potential for any conflict of interest and that the activities of the compliance function are subject to independent review.
- Review compliance functions itself or through Audit Committee of Board (ACB) or a specific Board level Committee constituted for the purpose, on a half yearly basis and annual review of status in implementation of compliance functions.
- Invite Compliance Officer to the meetings of the Board/ACB or a specific Board level Committee constituted for the purpose, wherein half yearly/ Annual review is undertaken.

b). Senior Management

Compliance is the function of the Bank as a whole. General Managers and the Deputy GeneralManagers in-charge of the corporate departments and Regional Heads and Head of theBranches shall be responsible for managing the compliance risk pertaining to their functional areas.

The bank's Senior Management with the participation of the Compliance Officer shall:

- Ensure that appropriate remedial action is taken if breaches are identified.
- The disciplinary action on such breaches is initiated in terms of “Discipline & Appeal Regulations”.
- Ensure that Compliance officer identifies & compiles list of compliance failure

and the concerned departments to formulate plans to mitigate such failures.

- Submit to the Board/ ACB/ Specific Board Committee constituted for the purpose, half yearly and annual reviews, and
- report promptly to the board of directors or the ACB or Specific Board Committee constituted for the purpose, on any material compliance failure (e.g. failure that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation).

7. Conclusion

Compliance function is to be fully cognizant of the “compliance risk” and the reputational risk arising out of compliance failures causing huge economic costs.

Compliance efforts can only succeed if all concerned work in harmony and maintain good mutual relationships with the aim to establish good compliance culture by understanding and performing the defined roles and responsibilities of compliance functionaries in various departments / offices / levels to catch “Noncompliance” in business.



Information Technology (IT) Risk

Bank already has an Information Security Policy in place. In this section Risks related to Information Technology (IT) are covered.

1. Introduction

These days technology enables virtually all the activities in the bank and consumes a huge portion of capital investment and operational expenses. The performance of the bank depends on the reliability and security of its technology. The bank's business relies on accuracy and timely availability of data. Weak controls in technology can lead to processing errors or unauthorised transactions.

The effective management and governance of IT risk depends both on the senior management team including the head of the IT department (the GM/ DGM in charge of IT) and the field functionaries across the bank.

2. Top IT Risk Defined

The main IT risk includes unauthorised access to systems, use, disclosure, disruption, modification, recording or destruction of customer and bank's data. Technology risk holds strategic, financial, operational, regulatory, and reputational implications.

Some of the most significant risks in technology in financial services include:

i). IT Environment Risk

- Regulatory Risk

ii). Strategic risk

- Organisation Risk
- Location Risk
- Technology vendor and third-party risk (Outsourcing Risk)

iii). Technology operations risk

- Data management risk including data disclosure risk

- IT resiliency and continuity risk (Interruption Risk)
- Product/ Services Risk

iv). Computer Fraud Risk

3. Risks and Control Measures

1. IT Environment Risk

- Regulatory risk includes non-compliance / violations of Regulations.
- Management of assets (Hardware) and software.
- Weak incident management.

Control Measure

- All IT products and services to comply with RBI and NABARD guidelines and regulations.
- All IT systems and procedures, products, and processes to comply with financial and business regulations.
- Data management capabilities should be as per regulatory guidelines.
- IT department should manage capacity, hardware, and software license agreements.
- Internal audit on the effectiveness of risk management and compliance functions of IT department may be carried out to provide assurances. The report may be put up to the senior management and the board.

2. Strategic Risk

- The IT systems and procedures are not aligned to the strategic objectives and business priorities of the bank.
- Location chosen for usage and storage of hardware may be susceptible to unforeseen events such as riots, floods, earthquake, and sabotage.
- There are outsourcing risks for data processing and data management.
- Poor management of the contract terms (with the suppliers/ vendors) can lead to disputes between suppliers and the bank.

Control measures

- The IT systems and procedures must meet the Strategic Objectives of the bank.
 - The head of IT department (GM / DGM -in charge) should be involved in the formulation of business strategy.
 - Business objectives and IT strategies should be aligned to avoid inappropriate investments and misaligned expectations.
 - Bank should periodically review the existing policies on IT strategy covering IT planning, resourcing, budgeting, future requirements, costs, and timelines.
 - The responsibilities and liabilities of vendors and customers should be clearly defined.
 - Over reliance on a single supplier should be avoided.

3. Technology operations risk

IT operations risk relates to those risks arising from day to day transaction processing on computer systems, data processing errors, interruptions.

- Data processing errors not being detected and corrected on a timely basis resulting in unreliable information.
- Unauthorised access to data on the computer system can put the bank to risk.
- Inadequate disposable techniques for hardware including CPUs, storage media such as disks, CD-ROMs etc., can lead to data falling into undesirable hands.
- Information System (MIS) fails to provide complete, accurate and timely information to the senior management for decision making.

Control Measures

- The branches and offices to ensure that data is correctly and accurately entered in the computer system.
- All transactions are accurately updated to the General Ledger and database files on day - to - day basis.
- IT department should exercise effective control over the data processes.
- Adequate contingency arrangements should be in place for difficulties faced in case of supplier, building and staff issues.
- Proper hierarchy to be advised to all staff members and field functionaries for

escalating system failures, staff shortages, vendor issues, software, and hardware related issues.

- Proper contracts to be drawn with the suppliers to avoid any disputes between the bank and the supplier.
- Due diligence must be performed on the vendors engaged by IT department for their reputation, financial viability, compliance, and other attributes.
- The IT department should regularly monitor the service delivery (by the vendors) against targets and timelines.
- Bank should conduct regular review of the location of IT resources to ensure that the location is appropriate.
- The disruption and/ or happening of any event prejudicial to the interest of the bank should be promptly reported to the head of IT department.
- Access to computer systems, servers should be restricted to authorised personnel only.
- The management should ensure that sufficient audit trails are designed into the system and there are security procedures around those trails so that they cannot be altered.

4. Computer Fraud Risk

- There are number of opportunities to fraudsters to commit fraud with ease and speed.
- The fraudsters can successfully hide their fraudulent activities for some time.
- There are risks associated when a new product or a process is implemented.

Control Measure

- Bank should have a system of generation of reports for detection and prevention of frauds.
- The access to computer terminals and files should be documented and strictly monitored.
- The incidence of occurrence of a fraud or a breach along with the measures adopted by the IT department should be promptly reported to the senior

management and the board.

- The modus operandi of operation of fraud to be shared with the field functionaries to avoid such incidents in future.

4. Emerging Products and Services

Internet Banking

Reserve Bank of India, vide its Circular No RBI/2015-16/229 dated the November 05, 2015, issued detailed guidelines on 'Internet Banking Facility for Customers of Cooperative Banks'. The revised guidelines for implementation by all cooperative banks cover:

- i. Technology and Security Standards
- ii. Legal Issues
- iii. Internal Control System

Third party transfer of funds through ATMs

RBI, vide its Circular No DBOD.No.BL.BC 5/22.01.001/2003 dated the July 23, 2003, allowed banks to provide the facility of transfer of funds from one customer's account to another customer's account of the same bank within the country, through ATMs.

'The mandate and related documentation which forms the basis for effecting payments for such transactions carried out over the ATMs should be settled bilaterally between the bank and customers and the rights and obligations of each party should be clearly stated in the mandate and should be valid in the court of law. The bank should take appropriate steps for securing discharge of their liability while permitting third party payments through ATMs.'

Mobile Banking transactions in India

RBI has issued 'Operative Guidelines for Banks' on mobile banking transactions in India. The banks must obtain RBI approval, (after seeking their Board approval), to start this facility for their customers. "Mobile banking transactions" is undertaking banking transactions using mobile phones by bank customers that involve credit/debit to their accounts.

Guidelines issued by RBI cover the following areas:

- i. Regulatory & Supervisory Issues
- ii. Registration of customers for mobile service

- iii. Technology and Security Standards
- iv. Inter-operability
- v. Clearing and Settlement for inter-bank funds transfer transactions
- vi. Customer Complaints and Grievance Redressal Mechanism
- vii. Transaction limit

RBI has also advised the ‘Technology and Security Standards’ covering the technology to be deployed and the security control to be exercised by the banks.

Banks are required to put in place appropriate risk mitigation measures like transaction limit (per transaction, daily, weekly, monthly), transaction velocity limit, fraud checks, AML checksetc. depending on the bank’s own risk perception, unless otherwise mandated by the Reserve Bank.

5. Roles and Responsibility of Board of Directors & Senior Management

- i. The Risk Management Committee may review the IT risks in the bank once in a year.
- ii. The focus of the Committee should be on traditional IT projects and IT risk events.
- iii. The Board may define certain thresholds that can come to their attention such as
significant IT investments, certain risk events such as cyber breaches, system outages, or regulatory notifications.
- iv. Board/ Senior Management may also consider laying down policy for career path and talent development in IT department.



Abbreviations Used	
ACB	Audit Committee of Board
AGM	Assistant General Manager
ALCO	Asset Liability Committee
BG	Bank Guarantee
CC	Cash Credit
CIBIL	Credit Information Bureau of India Limited
CM	Chief Manager
CORM	Committee on Operational Risk Management
CRAR	Capital to Risk (weighted) Asset Ratio
CRO	Chief Risk Officer
CRR	Cash Reserve Ratio
CTR	Cash Transaction Report
DGM	Deputy General Manager
FIU	Financial Intelligence Unit
GM	General Manager
HPSCB	HP State Cooperative Bank Ltd.
ICT	Information & Communication Technology
IRAC	Income Recognition, Asset Classification & Provisioning Requirements
KYC	Know Your Customer
LC	Letter of Credit
MD	Managing Director
MIS	Management Information System
NABARD	National Bank of Agriculture and Rural Development
NII	Net Interest Income
NIM	Net Interest Margin
ORMC	Operational Risk Management Committee
RBI	Reserve Bank of India
RM	Risk Management

RISK MANAGEMENT POLICY

RMC	Risk Management Committee
-----	---------------------------

RMD	Risk Management Department
RO	Regional Office
SARFAESI Act	Securitisation & Reconstruction of Financial Assets & Enforcement of Security Interest Act, 2002
SLR	Statutory Liquidity Ratio
STR	Suspicious Transaction Report
TL	Term Loan