केन्द्रीय कार्यालय
बालुवाटार, काठमाडौं
फोन नं. : ०१-५७१९६४१/४२/४३/४४
Website : www.nrb.org.np
पोष्ट बक्स : ७३

नेपाल राष्ट्र बैंक

बैंक तथा वित्तीय संस्था नियमन विभाग

पत्र संख्या : वै.वि.नि.वि./नीति/सूचना/१०/०८३/८४

मिति : २०८३/०५/२९

सूचना

इजाजतपत्रप्राप्त "क", "ख" र "ग" वर्गका बैंक तथा वित्तीय संस्थाहरु

महाशय,

यस बैंकबाट जारी गरिएको **"Risk Management Guidelines For Banks and Financial Institutions, 2018"** लाई अद्यावधिक गरी संलग्नबमोजिमको **"Risk Management Guidelines For Licensed 'A', 'B' and 'C' class Banks and Financial Institutions, 2026"** जारी गरिएको हुँदा सोहीबमोजिम गर्नु गराउनु हुन नेपाल राष्ट्र बैंक ऐन, २०५८ को दफा ७९ ले दिएको अधिकार प्रयोग गरी यो सूचना जारी गरिएको छ।

भवदीय,

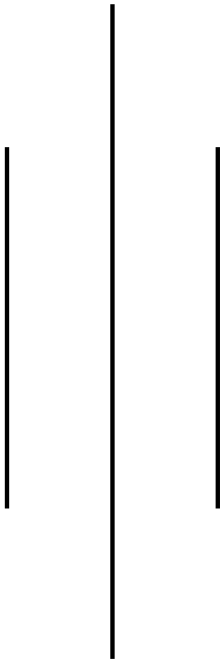
कार्यकारी निर्देशक

Risk Management Guidelines

For

Licensed 'A', 'B' and 'C' class

Banks and Financial Institutions



Nepal Rastra Bank

Banks and Financial Institutions Regulation Department

2026

Contents

List of Abbreviations

AI	Artificial Intelligence
ALCO	Asset Liability Management Committee
ALM	Asset Liability Management
AML	Anti-Money Laundering
BCBS	Basel Committee on Banking Supervision
BCP	Business Continuity Plan
BFIs	Banks and Financial Institutions
BOD	Board of Directors
CDD	Customer Due Diligence
CFP	Contingency Funding Plan
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIRT	Cybersecurity Incident Response Team
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
CTO	Chief Technology Officer
DRP	Disaster Recovery Plan
EaR	Earnings-at-Risk
EDD	Enhanced Due Diligence
ESRM	Environmental and Social Risk Management
EVE	Economic Value of Equity
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
GRI	Global Reporting Initiative
ICAAP	Internal Capital Adequacy Assessment Process
ICT	Information Communication Technology
IRRBB	Interest Rate Risk in the Banking Book
ISO	International Organization for Standardization
ISSB	International Sustainability Standards Board
IT	Information Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LCR	Liquidity Coverage Ratio
LTV	Loan to Value
MIS	Management Information System
ML/TF	Money Laundering/ Terrorism Financing
NFRS	Nepal Financial Reporting Standards
NII	Net Interest Income
NRB	Nepal Rastra Bank
NSFR	Net Stable Funding Ratio
ORM	Operational Risk Management
RCSA	Risk and Control Self-Assessment
RMC	Risk Management Committee

RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOL	Single Obligor Limit
TF	Terrorism Financing
TRM	Technology Risk Management
UNSC	United Nations Security Council
VRS	Voluntary Retirement Scheme

I - Risk Management Guidelines

1.1 Overview

Taking risk is an integral part of financial intermediation and banking industries in order to realize sustainable returns on their investments. On the other hand, risks assumed have the potential to wipe out expected returns and may result in losses for the institutions, which may endanger the soundness of individual financial institutions and affect the stability of the overall financial system. Hence, setting an appropriate risk management strategy, risk tolerance/appetite level and a holistic risk management approach with effective reporting lines to the senior management enables financial institutions to take risks knowingly and treat risks appropriately.

Risk management is a part of internal governance involving all areas of financial institutions. There is a strong link between good corporate governance and sound risk management. Without proper risk management, the various functions in a financial institution cannot work together to achieve the institution's objectives. It is an essential part in helping the financial institution grow and conserve sustainability and resilience.

The emergence of new risks to the financial sector continues to threaten global financial stability. Escalating climate change has prompted central banks, financial regulators and international supervisory bodies all over the globe to set out principles, guidelines and regulations for combating climate and environment-related risks. The rapid adoption of digitalization, increasing reliance on data-driven technologies, and advancement of cutting-edge innovations such as artificial intelligence (AI) have significantly enhanced the efficiency, accessibility, and innovation of the financial system. At the same time, these developments have introduced new and evolving risks related to data confidentiality, cyber security, operational resilience, and the safety and integrity of payment systems and financial markets. As financial institutions become more interconnected and technology-dependent, strengthening risk management frameworks is essential to harness the benefits of technological innovation while effectively managing the associated risks.

Following the global financial crisis, risk management in financial institutions has evolved from a compliance-driven function to a top-level comprehensive activity relevant at the highest levels of decision-making and strategy setting. While the extent of the risk management function performed and the structure kept in place depend on the size and complexity of individual financial institutions, risk management is most effective when basic principles and elements of risk management are applied consistently throughout the financial institution. Additionally, each financial institution should implement a comprehensive risk management program tailored to its needs and the circumstances under which it operates.

1.2 Scope and Objectives of the Guidelines

1.2.1 Scope

Nepal Rastra Bank has issued these guidelines to provide guidance to all financial institutions on minimum standards for risk management. These guidelines are not intended to be exhaustive. A financial institution may, depending on its size, complexity, level of risk exposure and interconnectedness with other financial institutions, establish a more advanced framework than outlined in this document. Financial institutions are in fact encouraged to self-assess their risk profile and operational context, and customize their risk management framework and approach to attain organizational goals while meeting the minimum requirements and standards set out in the guideline. While these guidelines provide a summary outline of risk management, financial institutions should

also adhere to the guidelines issued by global standard setters for prudential regulation, such as the BCBS and FSB (e.g., revisions to the principles of sound management of Operational risks, Framework for Internal Control Systems in Banking Organizations, the internal audit function in banks, the compliance functions in banks and so on).

This guideline provides guidance on the management of the major risks that financial institutions may face, namely: Credit Risk, Liquidity Risk, Operational Risk, Market Risk, Interest Rate Risk, Technology Risk and Climate Risk. However, financial institutions may, if deemed necessary, apply the guideline to all other risks that they are exposed to, in addition to the risks mentioned in the document.

1.2.2 Objectives

In publishing this guideline, the objectives of the Nepal Rastra Bank are:

a) To promote better risk culture at all levels of the financial institution.

b) To provide minimum standards for risk management practices.

c) To improve the financial soundness of individual financial institutions and the stability of the overall financial sector.

d) To encourage financial institutions to adopt and implement a sound risk management framework.

e) To introduce important risk management tools and techniques for assessment and necessary treatment of various risks.

1.3 Dimensions of Risk Management

1.3.1 Risk Culture

Every financial institution should develop an integrated and institution-wide risk culture, based on a full understanding of the risks it faces and how they are managed, considering risk tolerance and appetite. Since the business of financial institutions involves risk taking, it is fundamental that risks are appropriately managed. A sound and consistent risk culture throughout a financial institution is a key element of effective risk management. An institution will develop its risk culture through policies, examples, communication, and training of staff regarding their responsibilities for risk and every member of the financial institution should be fully aware of his or her responsibility regarding risk management. Additionally, risk management should not be confined to risk specialists or to control functions only. Business and operational units should be primarily responsible for managing risk on a day-to-day basis, and should consider risk tolerance and risk appetite (according to the format as specified in the Annexure of the Guideline), in line with the financial institution's risk policies and procedures.

Risk culture and its impact on effective risk management must be a major concern for the board and senior management. A sound risk culture encourages effective risk management, promotes sound risk-taking and ensures that risk-taking activities beyond the institution's risk appetite are recognized, assessed, reported, and addressed in a timely manner. Weaknesses in setting the risk culture are often the root cause of the occurrence of significant risk events, financial institution failures, and financial crises.

The Board of Directors (BoD) of the institution sets the tone for the desired risk culture. The risk culture can be strengthened through:

a) Enabling an open and respectful atmosphere in which employees feel encouraged to speak up when observing new or excessive risks;

b) Clarifying the range of acceptable risks using an embedded risk appetite statement and various forms of communication and training; and

c) Aligning incentives with objectives and clarifying how breaches of policies/procedures will be addressed.

1.3.2 Risk Strategy and Risk Appetite

Risk tolerance and risk appetite are terms often used interchangeably: Risk appetite means the aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan; risk appetite describes the absolute risks a financial institution is *a priori* open to take; while risk tolerance relates to the actual limits within its risk appetite that a financial institution pursues.

A financial institution's strategy details the long-term, and in some cases, short-term goals and objectives, as well as how progress toward their achievement is measured. Along with business goals, the financial institution must have risk goals and risk strategies that enable it to achieve the desired risk profile.

The board of directors sets the strategies and senior management is responsible for implementing those strategies and communicating them throughout the organization. The risk appetite statement plays an important role in cascading the risk strategy throughout the institution. It includes metrics and indicators concerning specific risk types. The risk-appetite statement should be well-embedded and be consistent with the firm's capacity to take risks, taking into consideration the capital constraints, potential profit and loss consequences and level of sustainable returns the institution expects to achieve for incurring various risks.

A good practice includes the following:

a) Regular review of risk appetite statement as a formal process;

b) Top-down and bottom-up processes to define risk metrics and risk appetite; and,

c) Limit systems that are aligned with overall governance so that breaches are quickly flagged and appropriate counter-measures are taken.

1.3.3 Risk Governance and Organization

Risk governance refers to the structure, rules, processes, and mechanisms by which decisions about risks are taken and implemented. It covers the questions about what risk management responsibilities lie at what levels and how the board influences risk-related decisions as well as the role, structure, and staffing of risk organization. A good practice in this dimension is characterized by the board regulatory engages with key risk issues with clearly defined risk management roles and responsibilities proportionate to the risks assumed at a particular organizational level or unit.

Risk governance should follow the three-lines-of-defense-model. The first line of defense ensures that the business and operation units of the institution have in place effective processes in place to identify, assess, measure, monitor, mitigate, and report on their risks. Each unit operates in accordance with the risk policies and delegated mandates. The units are responsible for having skills, operating procedures, systems, and controls in place to ensure their compliance with risk policies and mandates.

The second line of defense relates to the appropriate Internal Control framework put in place to ensure effective and efficient operations, including the following;

a) Adequate control of risks;

b) Prudent conduct of business;

c) Reliability of financial and non-financial information reported or disclosed (both internally and externally); and

d) Compliance with laws, regulations, supervisory requirements, and the institution's internal policies and procedures.

The Internal Control framework encompasses the risk control function and compliance function, and should cover the whole organization, including the activities of all business, support, and control units. The risk management unit, generally headed by a Chief Risk Officer, has the responsibility of recommending and monitoring the financial institution's risk appetite and policies, and for following up and reporting on risk-related issues across all risk types.

The third line of defense consists of the financial institution's internal audit, which performs independent periodic reviews of the first two lines of defense, provides assurance and informs the first two lines of strengths and potential weaknesses.

1.3.4 Risk Assessment and Treatment

The ultimate responsibility for risk assessment lies solely with a financial institution: it should evaluate its risks critically and not rely on external assessments.

The risk management process is the systematic application of management policies, procedures and practices to the assessment, treatment, controlling, monitoring, reporting and controlling or mitigating of risk. The process should be an integral part of management, be embedded in the culture and practices, and should be tailored to the business processes of the organization.

Regardless of the types of structure-maintained strategies formulated by the financial institution, the risk management process should include proper risk assessment and treatment as described below.

a) Risk Assessment

Risk assessment is the overall process of risk identification, analysis, and evaluation.

Risk identification is the starting point for understanding and managing risks and/or crucial activities. Institutions should identify the nature of risk, sources of risk, cost of risk, areas of impact, events, their causes, and their potential consequences. They must recognize and understand risks that may arise from both existing and new business initiatives. They should implement adequate tools and techniques to identify risk because those not identified at this stage will not be included in further analysis.

Risk analysis involves developing an understanding of the risk. It provides an input for risk evaluation and to decisions on the most appropriate strategies and techniques for risk treatment. The institution's risk analysis involves measuring risk by considering the consequences of an unfavorable event and the likelihood of occurrence of such events. Factors that affect consequences and likelihood should also be identified. Risk analysis can be undertaken with varying degrees of detail, depending on the nature of risk, severity of risk, and the information, data and resources available. Analysis should be quantitative and qualitative in nature. To the maximum possible extent, financial institutions should establish systems/models that quantify their risks; however, in some risk categories, such as

reputational and operational risks, quantification may be difficult and complex. When it is not possible to quantify risks, qualitative measures should be adopted to capture those risks.

Risk evaluation is undertaken to assist in making decisions, based upon the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Some risks need to be immediately addressed and should be brought to the immediate attention of the management body. Risk evaluation mainly involves comparing the level of risk found during the analysis process with the financial institution's risk appetite, risk tolerance level and regulatory limits. Based on this comparison, the need for appropriate treatment should be considered.

b) Risk Treatment

After the exposed risks are assessed, financial institutions should choose the best option to mitigate unacceptable risks. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following and can be applied either individually or in combination:

i) Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.

ii) Accepting and retaining the risk by making informed decisions and having plans for managing and funding the consequences of the risk if it occurs.

iii) Reducing the likelihood of the risk through staff training, changing procedures, or by reducing the impact through diversifying the credit portfolio, setting up off-site data backup, etc.

iv) Sharing the risk with another party or parties through insurance, consortium financing, etc.

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, regarding legal, regulatory, and other requirements.

One of the most important ways for financial institutions to address risks is to put in place adequate risk control mechanisms. The institution should establish and communicate risk limits through policies, standards and procedures that define responsibilities and authority. These limits will help the concerned parties know when the risk becomes unacceptable and align their actions and behaviors with the institution's set risk appetite, risk tolerance, and strategy.

Monitoring and review need to be integral parts of the risk treatment plan to ensure that measures remain effective. The institution's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

i) Detecting changing risk sources and factors within and outside the institution,

ii) Identifying emerging risks.

iii) Obtaining further information to improve risk assessment,

iv) Ensuring that controls are effective and efficient in both design and operation,

v) Analyzing and learning lessons from events, trends, etc., and

vi) Identifying emerging risks.

1.4 Risk Management Framework

A financial institution's risk management framework shall include in its foundation policies, procedures, limits, and controls. This foundation provides adequate, timely, and continuous identification, assessment, measurement, monitoring, mitigation, and reporting of risks posed by its activities at the business line and institution-wide levels.

The success of risk management in financial institutions will depend on the effectiveness of the risk management framework providing the foundation and arrangements that are put in place throughout the organization at all levels. The framework should be comprehensive enough to capture all the material risks to which the institution is exposed. It should facilitate processes for assessment and necessary treatment of these risks. The minimum standards of a sound risk management system include the following elements.

1.4.1 Active Board and Senior Management Oversight

The introduction of risk management and ensuring its ongoing effectiveness must come from the top level of the institution. As the board of directors has the ultimate responsibility for the risks taken by the financial institution, it must define the risk appetite and risk tolerance, and set risk strategies. It is responsible for understanding the nature of risks significant to the institution and for ensuring that management is taking necessary steps to implement those strategies and manage accompanying risks.

While the overall responsibility for risk management is recognized to rest with the board of directors, it is the duty of senior management to transform the strategies into operational policies, procedures, and processes for effective risk management. Senior management should be fully aware of the activities undertaken by the institution that could expose it to various risks. It should possess the necessary knowledge and skills to be able to align the risk levels with the board's strategies through risk assessment and treatment. Top management should be aware of the financial institution's risk profile on an ongoing basis and should regularly report it to the board or a board-level committee for review.

1.4.2 Risk Management Department(s) and Various Committees

Financial institutions must have an independent risk management department. As necessary, it may have separate risk management divisions or units within the risk department to oversee each key risk area. The main functions of the department/units include the following:

a) managing the process for developing risk policies and procedures,

b) coordinating with business users to prepare functional specifications,

c) preparing and forwarding risk reports, and

d) assisting in the implementation of all aspects of the risk function.

The risk management function should be functionally and hierarchically independent from business and other operational functions. The officials who take and own risks should not be given responsibility for monitoring and evaluating their risks. The Chief Risk Officer leading the independent risk management department should have sufficient stature, authority and seniority. The Chief Risk Officer should have direct access to the board of directors and should make direct reports to the board or its Risk Management Committee. Safeguards against conflicts of interest should be put in place to maintain independence of the risk management function.

The risk management function should be provided with sufficient resources. The risk management department should have a sufficient number of personnel who possess the needed experience and qualifications, including market and product knowledge and command of risk discipline. Likewise, adequate budget should be allocated to this function to enable it to carry out its crucial function effectively.

Depending on the size and complexity of the financial institution, various committees and sub-committees may be set up for monitoring and controlling risks. These include board-level committees such as the Risk Management Committee, Compensation Committee, and management-level committees such as the Credit Risk Management Committee and Asset Liability Management Committee (ALCO).

1.4.3 Policies and Procedures

The board of directors and senior management must formulate and implement risk management policies and procedures to deal with various risks that arise from the financial institution's business and operational activities. The financial institution's policies and detailed procedures should provide guidance for the day-to-day implementation of broad risk strategies, and generally should generally include limits designed to shield the institution from imprudent and unwarranted risks. These policies and procedures include not only those relevant to specific risk areas like Credit Policy, Liquidity Management Policy, and Operational Risk Management Policy, but also those related to overall risk management.

The board of directors should review risk policies, procedures, and limits in a timely manner and update them when necessary. Furthermore, the internal audit should provide independent assurance about the efficacy of these policies.

1.4.4 Appropriate Management Information System (MIS)

Effective MIS is necessary for adequate risk monitoring and reporting. An effective MIS to generate key risk indicators in the form of accessible reports in a timely manner, enables risk managers to monitor the risk levels continuously and inform senior management and the board as necessary or as required. For instance, these reports may include important statistics such as daily/ weekly liquidity gap reports and a list of loans of significance (troubled, large, maturing, etc.) The MIS should also be able to produce reports in accordance with regulatory requirements.

In addition to regular reporting, there should be a system to address any exceptions observed. Furthermore, there should be an explicit procedure regarding measures to be taken to address such deviations.

1.4.5 Comprehensive Internal Controls and Limits

Internal control plays a critical role in managing risks of a financial institution. With a comprehensive internal control structure in place, management will be better able to contain risks within the level commensurate with the institution's risk appetite, risk tolerance, and strategy. An effective internal control system enforces the official lines of authority and provides for appropriate separation of duties. A major part of the internal control structure is the establishment of limits such as limits on liquidity, officer limits, and limits on non-performing assets. These limits ensure that the financial institution's management does not take excessive risks while pursuing business targets.

The financial institution's internal control system should be adequately tested and reviewed by its internal audit, which must be independent of the audited activities. The audit function should be governed by the audit charter, should be well resourced and equipped with staff with professional competence. Financial institutions should avoid both frequent staff transfers (less than two to three

years) and over-reliance on a particular person in the audit function (more than five to seven years). Staff rotations to and from the internal audit function should be governed by and conducted in accordance with a sound written policy. The coverage, procedures, and findings of the audit regarding the internal controls should be adequately reviewed by the Audit Committee and any material weaknesses found should be addressed promptly and appropriately.

II – Credit Risk Management

2.1 Overview

Credit risk is the risk that a borrower or counterparty will fail to meet their obligations according to the agreed terms, resulting in economic loss to the financial institution. While loans are the largest source of credit risk, other sources of credit risk exist throughout the activities of a financial institution, including in the trading book, and both on and off the balance sheet.

Given the significant weight of the credit risk in the risk profile of banks and other credit institutions, robust arrangements for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating this risk (including counterparty credit risk) should be put in place. The effective management of credit risk is a critical component of a comprehensive approach to risk management. Appropriate governance, processes, and internal controls should exist for accepting, managing and monitoring credit risk, on a group and solo basis, in a manner commensurate with the nature, scale and complexity of the financial institution's activities. Financial institutions must have sound procedures for valuing their credit exposures, which requires the existence of updated provisioning policies. They should have a forward-looking perspective to evaluate whether the arrangements in place are adequate to cope with the credit risk they might be exposed to in the foreseeable future.

In this section, the components of an appropriate credit risk management: organizational structure; credit strategies, policies, and procedures; limits and indicators; credit granting process; credit administration, measurement and monitoring processes; credit risk mitigation techniques; and controls of credit risk are discussed.

2.2 Appropriate Organizational Structure

a) Organizational structures vary according to the size, complexity and diversification of financial institutions' activities. However, whatever the structure in place, it must facilitate effective management oversight and proper execution of credit risk management and control processes.

b) There should be segregation of duties regarding various credit-related functions, such as credit assessment, analysis, approval, disbursement, administration, and monitoring. For large banks, different units should be established to perform each function. However, in smaller banks where it may not be possible to adequately staff different units, the structure in place should ensure that conflicts of interest between these functions are identified and managed and that sufficient checks and balances are in place even if they are within the same unit.

c) Banks should have a Credit Risk Management Function independent of the risk-taking units. This Credit Risk Management Function should have the power to challenge and, if necessary, escalate its concerns to senior management regarding the development of the credit risk management framework. This function should be separated from other credit-related functions and must be kept under the Chief Risk Officer, or a similar authority or person (second line of defense).

2.3 Credit Risk Strategies, Policies and Procedures

a) The credit risk strategy should include an assessment of the credit risk profile of the bank and a statement of the bank's appetite to take credit risk for each activity type, product type (such as working capital, consumer loan, fixed-term, etc.), economic sector (such as real estate, construction, retail), geographical location, etc. The credit risk strategy should be communicated throughout the organization and periodically reviewed at board or management level.

b) The credit strategy should include the identification of target markets and overall characteristics that the bank would want to achieve in its credit portfolio, including levels of diversification and concentration tolerances. The strategy should not consider only target markets but be developed based on the internal strength of the organization. Finally, the credit risk strategy should provide continuity in approach and consider cyclical aspects of the country's economy, the resulting shifts in composition and quality of the overall credit portfolio and forward-looking information in the market.

c) There should be policies in place regarding the information and documentation needed to approve new loans, renew existing ones and/or change the terms and conditions of previously approved credits.

d) For each type of loan, credit policies and procedures should define criteria for granting loans safely and soundly, including, but not limited to:

   i) Purpose of credit, assessment of future cash flows and other sources of repayment,

   ii) Collection of relevant information based on the different client risk profiles,

   iii) Use of adequate tools such as scoring or internal rating systems,

   iv) Analysis of borrower's repayment history (including, when possible, that in other banks), as well as current and future capacity to repay, based on historical financial trends and future cash flow projections,

   v) For commercial credits, the borrower's business expertise and the condition of the borrower's economic sector and its position within that sector

   vi) Net worth of the borrower and personal guarantors,

   vii) The proposed terms, conditions, and covenants of the credit agreement,

   viii) Collateral and its sensitivity to economic and market developments,

   ix) Adequacy, enforceability, and liquidity status of collaterals, as well as the practical aspects of their mobilization.

e) Credit policies must address credit risk in all the bank's activities, at both individual and portfolio levels. Such policies should be clearly defined, consistent with the credit strategy, comply with regulatory requirements, international standards and banking practices, and be adequate for the nature and complexity of the bank's activities.

f) Policies and procedures should clearly specify the diverse types of loans, the actions the concerned staff of various functions involved must take to evaluate and approve the credit proposals, and monitor credit relationships.

g) Credit policies must include clear provisions regarding credit approving authority, defining delegations and exceptions or waivers, and their implementation. Delegation of authority must always be clearly spelled out, considering knowledge and experience.

h) Bank must have a well-defined policy regarding collateral, including types of collateral accepted, haircuts, and maximum loan-to-value (LTV) for each type of product in relation to the collateral.

2.4 Credit Limits and Indicators

a) To ensure diversification of risks and limit concentration risk, limits on credit exposures should be set for all relevant activities. They may include:

   i) Limits on exposure to specific activities or type of products, including off-balance sheet products;

   ii) Limits on single counterparties and groups of connected counterparties, including other banks and financial institutions, domestic and foreign;

   iii) Limits on specific industries and/or economic sectors/ sub-sectors;

   iv) Limits on exposure to types of collateral;

   v) Limits on exposures to related parties;

   vi) Limits on branches and/or exposures to geographic regions, including other countries;

   vii) Limits on the credit that may be granted by approving managers.

   viii) Limit on non-performing assets/loan

   ix) Limit on loan-to-value ratio

b) These limits should be reviewed and updated periodically, and at least once a year. In addition, banks should consider the results of stress testing in the overall limit setting and monitoring process.

c) In addition to setting limits, banks should use early warning indicators to signal at an early stage where there is increased exposure to specific components of credit risk, and should respond to these indicators by assessing whether they point to potential problems in credit quality.

2.5 Credit Granting Processes

Granting of credit should follow pre-determined processes:

a) **Assessment:** credit proposal assessments should be performed at the relevant level according to the bank's organization and structure. Credit assessment should follow procedures, methodology and operating guidelines describing the necessary nature and extent of due diligence and collection of relevant supporting documents and information based on their risk profiles.

b) **Review:** before submitting credit proposal assessments to the approving person, unit and/or committee, the bank should undertake a review and analysis of loan proposals by a person, including thorough analysis of risk profile and characteristics of the borrower or counterparty, source of repayment, purpose and structure of credit, etc., independent from the initial assessment. While the credit risk management department/unit should generally be given responsibility to conduct such review, in smaller organizations an independent review could be done by any appropriate official not involved in the credit appraisal and approval process.

c) **Approval:** the designated level of approving authority takes the approval decision, including the approval of specific terms and conditions, based on the initial credit assessment, independent review and analysis.

d) **Disbursement:** following the notification of the approval decision, disbursement is made by the designated unit/person, following procedures to ensure that all terms and conditions are verified and guarantees, if any, are taken.

e) **Administration:** the credit administration function is responsible for utilization and monitoring of disbursed credits, maintaining credit files and ensuring they are kept up to date, and for follow-up on necessary actions (renewal notices, updating information, etc.).

2.6 Credit Risk Monitoring

a) Monitoring of credit risk should be performed by the Credit Risk Management Function without any influence of the risk-taking units.

b) Financial institutions should have in place a methodology to adequately classify their credit risk, at institution, portfolio and borrower level. The classification of the credit risk should use quantitative and qualitative criteria, follow a graduation of the different level of inherent risk, with appropriate actions consistent with the level of risk identified.

c) A valuable tool in monitoring the quality of individual loans, as well as the total portfolio, is the use of internal rating systems (IRR) which helps the financial institution to differentiate between different credit exposures in its portfolio, determine the portfolio's characteristics (concentration, problem loan, etc.) and verify the accuracy of the provisions.

d) Banks should monitor the quality of the credit relationships on an ongoing basis and keep updated information on their credit portfolios, and on the risk profiles and situation of the borrowers. This includes timely collection and regular review of financial information, including audited annual financial statements.

e) Business borrowers should also be monitored through on-site visits, while repayment capacities of individual customers should be updated regularly for early identification of any adverse developments that may affect repayment of loans.

2.7 Remedial actions

Banks should have effective processes and procedures in place for early implementation of remedial actions on deteriorating credits and management of problem loans. Once a loan shows signs of weakness, it should be managed through a dedicated remedial or workout process. Key elements include:

a) Maintaining frequent contact with borrowers and keeping proper records of follow-up actions.

b) Taking timely remedial measures such as additional collateral/guarantee, rescheduling, restructuring or other workout plans based on business condition, borrower viability, and his/her commitment and willingness to repay the loan.

c) Ensuring that restructuring or rescheduling is not used merely as forbearance and is approved by the competent authority with proper justification.

d) Updating collateral valuation and reviewing security documents to ensure enforceability of contracts, collateral and guarantees.

e) Conducting more frequent review and monitoring of problem loans, including progress of remedial plans.

f) Reporting the status and progress of problem loans to senior management timely.

2.8 Recovery process

a) When rescheduling and restructuring are not options or fail to improve the situation, problem loans should be dealt with by a specialized recovery unit. This unit should make proactive efforts in dealing with problem borrowers.

b) When all efforts fail, banks should write off loans and liquidate collateral to minimize cost.

c) Such process should be strictly monitored, require a specific level of approval, and specific information to the board and the NRB.

2.9 Provisioning Process

Banks should have a well-documented loss provisioning methodology, including credit risk assessment policies, procedures and controls for identifying problem loan exposures and determining loss provisioning in a timely manner, also in accordance with NFRS 9- Expected Credit Loss Related Guidelines, 2024.

III – Liquidity and Funding Risk Management

3.1 Overview

Liquidity risk is the risk that a financial institution loses its ability to fund its assets or to meet its obligations as they come due without incurring unacceptable costs or losses.

Liquidity risk encompasses various aspects:

a) Intraday liquidity risk is the risk that the financial institution becomes unable to settle its financial obligations in due time during the day;

b) Funding liquidity risk is the risk arising from the inability to raise adequate funds in a timely and cost-effective manner to meet lending or investment needs. Funding liquidity risk arises from a maturity gap between assets and funding, resulting from the maturity transformation embedded in commercial banking business.

c) Market liquidity risk is the risk that a financial institution cannot easily cover its liquidity needs by liquidating a position through securities lending or selling at the market price because of inadequate market depth, price deterioration or market disruption. Market liquidity risk materializes in asset and derivative markets;

d) Funding cost risk is the risk that a financial institution can replace maturing funding only at higher costs to fund its assets.

Virtually every financial transaction or commitment has implications for a bank's liquidity risk. Unstable deposits or unexpected withdrawals of deposits are a major cause of liquidity risk. Unplanned expansion of credit may also be a source of such risk. Further, off-balance sheet commitments and other contingent liabilities, including undrawn loan commitments, may have a serious impact on a bank's liquidity risk.

From a management point of view, under the oversight of the Asset-Liability Management Committee (ALCO), the funding liquidity risk is split between short-term liquidity risk (up to one year with a strong focus on the period up to one month) which is generally managed by the treasury department and/or the treasury committee of the financial institution, and long-term liquidity risk (beyond one year) which is generally managed by the asset liability management (ALM) department.

There are no specific ratios covering the periods under one month, between one month and one year, or intraday liquidity, but financial institutions should monitor their liquidity and funding positions over the whole spectrum of maturities from the shortest to the longest.

For effective liquidity risk management, a financial institution needs an appropriate organizational structure; strategies, policies, and procedures; limits and indicators; and monitoring and reporting mechanisms. In addition, it will need an adequate information system to ensure effective monitoring of its liquidity, including a cushion of unencumbered, high-quality liquid assets, to withstand a range of stress events, including those involving the loss or impairment of both secured and unsecured funding sources.

3.2 Organizational Structure

a) The liquidity risk management and control functions should be part of an organizational framework with clearly defined tasks and responsibilities, including those units or committees that

are integrated in the monitoring and decision processes in charge of reviewing the risk profile and approving the risk strategy and appetite.

b) To establish a robust liquidity risk management framework, a bank should put in place organizational structure that is well integrated into bank-wide risk management process and is based on the three lines of defense approach.

c) The Liquidity Risk Management function is involved in daily monitoring of liquidity risk levels, timely reporting of important liquidity risk related information, and plays crucial part in the development of liquidity risk management policies. It should be independent and directly report to the CRO.

d) The Asset-Liability Management Committee (ALCO), usually a senior management committee that comprises the managers of the liquidity risk taking units and oversights both the short-term and long-term liquidity risks, should periodically report to the board.

3.3 Strategies, Policies and Procedures

a) Considering its risk profile, a financial institution should establish a liquidity risk management strategy that is customized to its institutional structure, organization, activities, products, and customers. The strategy should outline the targeted mix of assets and liabilities with clear implications for liquidity risk. Banks relying more on wholesale funding should maintain a relatively higher proportion of unencumbered, high-quality liquid assets than those banks that rely primarily on retail funding. If significant, the intra-day liquidity risk management requires specific attention.

b) The assessment of its own liquidity risk position and profile by the financial institution is the first step for defining the liquidity risk strategy and risk appetite and to build up a consistent liquidity management and liquidity risk management system. This assessment of the risk profile, risk strategy and risk appetite should be formalized in qualitative and quantitative terms, considering forward-looking aspects with regard to potential risks as well as changes in business strategies.

c) The liquidity risk strategy could in particular include the actual and targeted liquidity position, for example a maximum loan-to-deposit ratio or a maximum liquidity (and funding) market dependence. Under such strategy, financial institutions should also conduct stress testing under different stress scenarios. As a part of liquidity risk management strategy, the financial institution should regularly conduct liquidity gap analysis.

d) As a part of liquidity risk management strategy, a bank should have funding strategy that provides effective diversification in the sources and tenure of funding. A financial institution needs to monitor large borrowers and sectoral exposures by considering the liquidity risk implications.

e) A financial institution needs to study its deposit base in relation to diversification, maturity, and structure. It should also identify alternative sources of funding that strengthen its capacity to withstand a variety of severe institution-specific and market-wide liquidity shocks. Potential alternative sources of funding may include:

   i) New issues of short-term and long-term debt instruments,

   ii) Drawing down line of credit with other banks,

iii) Borrowing from the central bank,

iv) Lengthening of maturities of liabilities,

v) Repo of unencumbered, highly liquid assets,

vi) New capital issuance, sale of subsidiaries.

f) Policies and procedures should clearly define and describe risk management tools that the financial institution plans to use for assessment, monitoring and control of its liquidity risk. The steps involved in these tools should be documented and communicated throughout the organization. The policies should also include measurements of liquidity risk. In the future, financial institutions may use metrics such as Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR).

g) Policies should include clear definition of roles and responsibilities of individuals and teams performing liquidity risk management functions, including structural balance sheet management, pricing, marketing, management reporting, lines of authority and responsibility for liquidity decisions.

3.4 Limits and Early Indicators

a) To control its liquidity risk exposure and vulnerabilities, a financial institution should set limits on concentration of funding by counterparty, product type, currency, geographic market, etc.

b) Limits should be used for managing day-to-day liquidity within and across the business lines both under normal and stress conditions. While assessing how limits would perform under stressed conditions, a financial institution should include measures aimed at ensuring that it can continue to operate in a period of market stress, institution-specific stress and/or a combination of two.

c) A financial institution should also design a set of indicators to aid this process to identify the emergence of increased risk or vulnerabilities in its liquidity risk position or potential funding needs. Such early warning indicators should identify any negative trend and cause an assessment and potential response by management in order to mitigate the bank's exposure to the emerging risk.

d) Early warnings can be qualitative or quantitative in nature and may include (but not be limited to):

i) Rapid asset growth funded by unstable large deposits,

ii) Growing concentrations in either assets or liabilities,

iii) Deterioration in quality of credit portfolio,

iv) Significant deterioration in earnings performance or projections,

v) Increasing retail deposit outflows,

vi) A large off-balance sheet exposure,

vii) Deteriorating third party evaluation (negative rating) about the financial institution and negative publicity,

viii) Unwarranted competitive pricing that potentially stresses the financial institutions.

3.5 Measurement and Monitoring

a) A financial institution should employ a range of customized measurement tools, or metrics, as there is no single metric that can comprehensively quantify liquidity risk. To obtain a forward-looking view of liquidity risk exposures, it should use metrics that assess the structure of the balance sheet, as well as metrics that project cash flows and future liquidity positions, taking into account off-balance sheet risks.

b) The risk measurement tools should include vulnerabilities across normal and stressed conditions over various time horizons. Under normal conditions, prospective measures should identify needs that may arise from projected outflows relative to routine sources of funding. Under stress conditions, prospective measures should be able to identify funding gaps at various horizons.

c) Liquidity gap analysis involves a critical role for assumptions in projecting future cash flows. A financial institution should take steps to ensure that its assumptions are reasonable and appropriate, documented and periodically reviewed, tested and approved. The assumptions of duration of demand deposits, revolving type loans, and other off-balance sheet items with uncertain cash flows and the availability of alternative sources of funds during times of liquidity stress are of particular importance.

d) A financial institution should have a reliable management information system designed to provide forward-looking information on the liquidity position of the bank to the board of directors, senior management and other appropriate officials with timely. Further, the banks should have a set of reporting criteria, specifying the scope, manner, and frequency of reporting for various recipients (such as the board, senior management, ALCO) and the parties responsible for preparing the reports.

3.6 Reporting

a) Timely and adequate reporting of risk-related information is especially important for effective liquidity risk management. The top-level management should be able to easily look at the flash reports related to liquidity risk from the financial institution's MIS itself. The management must decide on the different reports (including regulatory reports) that are to be forwarded to the board and/or senior management and the frequency of such reporting. Further, the major issues discussed and decisions made in the ALCO meetings should also be forwarded to the board-level risk management committee.

3.7 Contingency Funding Plan

a) A Contingency Funding Plan (CFP) is a set of predefined processes, actions and measures to be taken in case liquidity risks materialize. Contingency plans are designed to address short-term liquidity shortfalls in emergency situations such as those envisaged in stress scenarios. Therefore, they only have a real value if they are anchored in the liquidity management and operational framework of the group, are regularly tested and reviewed, define responsibilities and contain a set of practical actions. They must be regularly reviewed and updated regularly to reflect changing market conditions, the business and risk profile of the bank.

b) Financial institutions must design and implement the CFP to meet funding needs under stress scenarios. Normally reliable funding can be seriously disrupted when put under stress. Hence, such funding plan is crucial for the financial institution's sustainability. CFPs should be commensurate with the financial institution's complexity, risk profile, scope of operations and role in the financial systems in which it operates. CFPs should include a clear description of a diversified set of viable, readily available and flexibly deployable potential contingency funding measures for preserving liquidity and addressing cash flow shortfalls in various adverse situations.

c) When developing a liquidity contingency plan, financial institutions should consider two types of liquidity crises: idiosyncratic, related to a liquidity problem in the financial institution itself, and market-wide, related to a liquidity crisis involving entire financial system.

IV – Operational Risk Management

4.1 Overview

Operational Risk is the risk of direct or indirect loss, or damaged reputation resulting from inadequate or failed internal processes, people and systems or external events. Operational risk has always been inherent to financial institutions and exists in all their activities.

Operational risk is a broad field and can be sorted into numerous sub-categories, such as IT risk, outsourcing risk and operational risk in market activities.

a) The major sources for operational risk are:
   i) Inadequate procedures and controls,
   ii) External and Internal frauds,
   iii) IT related activities and system failures,
   iv) Damage to physical assets,
   v) Execution, delivery, and process management
   vi) Third party dependencies
   vii) Human Resource Practices and workplace safety
   viii) Change in nature of job

b) Effectively managing operational risk requires:
   i) Identification and assessment of the operational risk inherent in all material products, activities, processes and systems,
   ii) A governance structure, effective governance in practice and a decision-making process for operational risk issues,
   iii) Strong corporate culture guided by corporate ethics and morale, ethical training to staffs, reward for high ethical performance
   iv) A definition of operational risk appetite which is consistent with the risk strategy,
   v) A documented and effective organizational framework for operational risk management with an adequate segregation of functions between risk-taking units and operational risk controls units and clear assignment of tasks and responsibilities,
   vi) An independent Operational Risk Management function,
   vii) Adequate and effective human and technical resources available for the functions involved in operational risk management and control,
   viii) An effective reporting system,
   ix) Contingency planning for addressing failures due to operational risks.
   x) Change management and building operational resilience

xi) Effective Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) measures, including customer due diligence, suspicious transaction monitoring, sanctions compliance, and reporting mechanisms, to mitigate compliance risk and reputational risk associated with ML/TF threats.

4.2 Organizational Structure

a) Financial institutions should develop a clear operational risk governance structure with well defined, transparent and consistent lines of responsibility. The governance structure should be commensurate with the nature, size, and complexity of the activities undertaken by the financial institution. However, in all cases, the operational risk governance function should be fully integrated into the financial institution's overall risk management governance structure.

b) A sound operational risk management structure should rely on three lines of defense: the business line management, an independent Operational Risk Management function, and internal audit. How these three lines of defense are implemented in practice will vary according to the size, business and risk profile of the financial institution. Nonetheless, the three lines of defense should, at minimum, cover the following aspects related to operational risk management:

   i) The business line should be responsible for identifying and managing risks inherent in the products, activities, processes, and systems for which it is accountable.

   ii) The Operational Risk Management (ORM) function is mainly responsible for independent review of processes put in place to control operational risk, and for measurement and reporting of the operational risk. In larger financial institutions, the ORM function will also be responsible for design, maintenance, and ongoing development of the operational risk framework. This function should directly report to the chief risk officer of the financial institution. The operational risk management framework should, at minimum, cover the following aspects:

      1. Governance structure, policies and procedures; risk appetite and tolerance; risk identification and control tools

      2. Inventory of risk and control, risk reporting and common taxonomy of operational risk terms

      3. Ensure independent review and focus on whether the operational risk management tools, such as risk and control self-assessments (RCSAs), key risk indicators (KRIs), issue and incident management, scenario analysis, comparative analysis, benchmarking etc. are being used meaningfully or implemented consistently by aligning actual risks and operations of the unit.

   iii) The internal audit should focus on providing independent assurance to the Board regarding the overall adequacy and appropriateness of the operational risk management framework and the governance processes.

c) The BODs and Senior Management of financial institutions should fulfill the following responsibilities for the management of operational risks:

   i) The BODs should approve and periodically review the operational risk management framework and operational resilience approach.

ii) The BODs should ensure that the senior management implements the policies, processes, and systems of the operational risk management framework and operational resilience approach effectively at all decision levels.

iii) The BODs should approve and periodically review risk appetite and risk tolerance for operational risk, focusing on the nature, types, and levels of operational risks that the bank is willing to assume. The risk appetite and tolerance level should be consistent with short-term and long-term strategic and financial plans of the financial institution.

iv) Senior management should articulate a clear and effective governance structure with well-segregated roles and responsibilities.

v) Senior management should be responsible for implementing, updating, and enforcing organization's policies, processes, procedures, and systems for managing operational risk, embedded in all material products, activities, processes, systems and consistent with the risk appetite and risk tolerance level.

vi) Senior management should formulate and implement business strategies, considering the results of operational risk assessment.

vii) Senior Management should implement code of conduct and ethics policy for all staff and get them attested by staffs on a periodic basis.

viii) Senior management should plan and implement training and development programs for all employees, segmented based on roles, responsibilities, and the nature of job.

4.3 Strategies, Policies and Procedures

a) Based on the financial institution's risk profile, the operational risk strategy must clearly articulate the nature, types, and levels of risk that the institution is willing to take (risk appetite). While formulating the strategy, the board must understand not only the level and complexity of risks inherent in the financial institution's activities, products, services, and systems, but also the expected outcome of not undertaking certain activities or systems. The operational risk strategy should take into account forward-looking aspects with regard to potential risks as well as changes in business strategies.

b) Operational risk policies and procedures should include all the relevant operational risk areas and establish a minimum set of operating instructions to have an effective risk management. They should be adequately documented, regularly updated, and available to all relevant staff. These policies and procedures should be aligned to the overall strategy and should support continuous improvement of risk management. They should be periodically reviewed by the senior management.

c) Policies should clearly define operational risk and related losses. Financial institutions that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their framework.

d) These policies and procedures should describe the risk assessment tools and how they are used. Further, they must provide for a common taxonomy of operational risk terms to ensure consistency of risk assessment, measurement, and reporting.

e) There must be different policies and procedures for undertaking existing and new activities. There should be tests and more rigorous assessments before undertaking new activities such as launching a new product or opening a new branch.

f) The operational risk policies should include clearly assigned authority, responsibility, and reporting relationships to encourage and maintain accountability.

g) The operational risk policies should focus on strengthening the operational resilience of financial institutions. Operational resilience should be explicitly included in the charter of the Risk Management Committee, and the decisions of BODs should be based on due consideration to operational resilience.

h) For building operational resilience, the operational risk policies should devise risk appetite and risk tolerance for disruption of critical operations and operational capabilities. For this, a clear segregation of critical from non-critical operations is vital in the operational risk policies.

i) Financial institutions should develop risk tolerance matrix for each critical operation. Such a matrix should be approved by the BOD. Such matrix can be time-based or based on service level. Nonetheless, it should qualify and quantify, as far as possible, the maximum acceptable level of disruption.

j) Financial institutions should map interdependencies and interconnections, creating spillover and dependency risks in the overall operations of critical services. Such a mapping should define the people, technology, processes, information, facilities, incentives, and interdependencies, including third party dependencies, needed to deliver critical operations.

k) Following the merger and acquisition policies, financial institutions that have merged or have acquired other financial institutions should duly incorporate well-being of human resources in their joint operations. Employee lay-off, voluntary retirement service (VRS), benefits and incentive plan, skill gap fulfillment, among others, should be proportionate and non-discriminatory.

4.4 Assessment and Measurement

a) Financial institutions must identify and assess the operational risk inherent in all products, activities, processes, and systems. The business line should assess for itself the relevant operational risks in their operations considering both internal and external factors. The second line of defense should challenge the business line's inputs to and outputs from, the financial institution's risk management systems.

b) To ensure an adequate risk management framework based on their specific situation, historical observations and internal assumptions, financial institutions should quantify their operational risks and not only rely on standard calculation.

c) The financial institutions must systematically track and record all relevant operational risk data, such as frequency, severity, operational risk losses, and other information on individual loss events or near misses. Analysis of loss events and near misses provide insight into the causes of large losses and information on whether control failures are isolated or systematic. It is also useful to monitor operational risk events affecting other financial institution, as far as available and relevant. Such data may be helpful for predicting future events and losses.

d) Business Process Mapping tools should be used for operational risk assessment: identification of key steps in business processes, activities and organizational functions, can reveal individual risks, risk interdependencies, and areas of control or risk management weaknesses.

e) Scenario analysis are also useful tools to assess operational risk, by obtaining expert opinion of business lines and risk managers to identify potential operational risk events and assess their potential outcome.

f) Specific attention should be devoted to low-frequency high-severity operational risk events (e.g. major fraud, bribery, etc.) which could deserve a specific process, in particular with regard to the timely information of the top management.

g) For operational resilience, the following assessment and measurement considerations should be ensured by financial institutions:

   i) Conduct third-party due diligence to include resilience assessment, contingency plan and other party assessment.

   ii) Implement business continuity planning and physical infrastructure in accordance with risk appetite and contingency scenarios.

   iii) Continuously improve crisis and incident response mechanism and recovery plans based on learnings from previous incidents, drills, simulation exercises.

   iv) Empower the crisis management team with authority to put forth internal controls following contingencies and external reporting and communication.

   v) Fully integrate Information communication technology (ICT) and cybersecurity risk management with overall operational resiliency plan, policies, and procedures.

4.5 Monitoring and Reporting

a) Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Regular monitoring enables timely detection and correction of deficiencies in procedures, controls, and systems, thereby substantially reducing the frequency and severity of risk events.

b) Operational risk management and monitoring require an adequate internal reporting framework for making regular reports to the appropriate levels of the institution, to inform the senior management and the board on the implementation of the risk strategy and the extent to which the risk appetite is reflected in actual risks being taken by the financial institution. The reports should be comprehensive, accurate, consistent and actionable across business lines and products.

c) The reporting on operational risk should be adequately structured to meet the needs of the appropriate management levels and of business and control units.

d) Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making.

e) Operational risk reports should include:

   i) Monitoring indicators;

ii) Breaches of the bank's risk tolerance level;

iii) Details of recent significant internal operational risk events and losses; and,

iv) Relevant external events and any potential impact on the financial institution and capital.

4.6 Contingency Planning

a) The partial or complete failure of one or several critical business processes or products represents a material operational, as well as reputational risk, for any institution. Planning is required for the actions which the bank may take in response to failures.

b) Contingency Planning refers to the set of predefined processes, actions and measures to be taken in case significant operational risks materialize, to enable the financial institution to face emergency situations. It should be implemented especially for all high-severity operational risks, which have the potential to disrupt the daily business or threaten the existence of the institution.

c) Business Continuity Management relates to the measures to ensure that critical business processes can be continued in the event of an emergency and the activities necessary to return to business as usual levels. IT continuity management is an integral part of the Business Continuity Management.

d) Business Continuity Plans (BCP) describe plans that allow an organizational unit's time-critical activities and business processes to restore operational status in the event of an emergency. The BCP defines strategies and options for various scenarios relating to a specific area and its processes. The BCP should identify all time-critical activities, business processes or resources and determine their maximum tolerable downtimes.

e) Plan should be tested periodically to ensure that they are likely to be effective in case of need.

4.7 Money Laundering (MF) / Terrorism Financing (TF) Risk Management

a) Money laundering and terrorist financing pose significant risks to banks, potentially leading to regulatory penalties, legal consequences, financial losses, and reputational damage. While ML/TF risk is generally considered a subset of operational risk, its broad and systemic implications demand dedicated focus and robust risk management. Therefore, the risk management policy approved by the Board should explicitly include ML/TF risk with defined roles, responsibilities, and reporting lines for its identification, assessment, customer due diligence (CDD) and enhanced due diligence (EDD), ongoing transaction monitoring, and mitigation in alignment with ML/TF Risk Assessment Guidelines for Bank and Financial Institution, 2022 issued by Nepal Rastra Bank.

b) Banks shall adopt a risk-based approach to AML/CFT compliance, integrating customer, product, delivery channels and geographic, and transactional risk factors. It should ensure that ML/TF risk is incorporated into the bank's organization wide risk assessment, internal audit coverage, internal capital adequacy assessment process (ICAAP), risk appetite statements, and training and awareness. Also, it must have strong transaction monitoring system for red flags detection in customers' transactions and report suspicious transactions to FIU-Nepal. Furthermore, use of machine learning and artificial intelligence should be encouraged.

c) The Board and senior management shall receive periodic reports on ML risk exposures, emerging typologies, and compliance status. Banks must maintain robust internal controls and systems to detect, report, and mitigate the ML/TF risks in line with national regulations including mechanism

for complying with Guideline on Targeted Financial Sanctions for Financial Institutions issued by NRB so as to comply with relevant provisions of United Nations Security Council (UNSC) resolutions and international standards including the FATF Recommendations, Basel Committee guidelines.

V – Market Risk Management

5.1 Overview

Market risk is defined as the risk of losses resulting from movements in market prices that adversely affect the value of on and off-balance-sheet positions of financial institutions. Financial institutions may be exposed to market risk in a variety of ways. Market risk takes various forms:

a) Foreign exchange risk, commodities risk throughout the institution,

b) Position risks arising from risk of losses due to changes in interest rates affecting the market value of tradable securities (e.g. bonds, treasury bills).

c) Equity risk is the risk of loss from changes in stock prices or stock market indices.

d) Concentration risk in the trading book as well as in the banking book.

Foreign exchange risk is the risk of losses arising from the movement of foreign currency exchange rates. While foreign exchange risk is categorized separately from other types of market risk in the NRB Directive, its management should follow the same structure and mechanisms.

Commodities risk is the risk of losses due to positions in commodities and trading in commodities-related financial instruments. It includes basis risk, forward gap risk etc. It incorporates variations in the "convenience yield" between derivatives positions, such as forwards and swaps, and cash positions in the commodity.

Position risk is the risk of loss on debt or equity instruments held in the trading book. A distinction should be made between debt instruments and equity instruments. Debt instruments are subject to general interest rate risk (related to maturity or duration of an instrument) as well as to specific interest rate risk in trading book (risk of losses resulting from changes in the creditworthiness of the single issuer). Equity instruments are subject to a general market risk component (i.e. the risk of losses caused by changes in the whole market) and specific market risk component (i.e. the risk of losses caused by price movements related to a single issuer).

Concentration risk relates to concentration and correlation factors in market transactions (not captured throughout the broader analysis of credit concentration risk). Financial institutions should assess if there is a concentration of instruments that may react in the same manner to a specific market event. It should also be pointed out that net positions may potentially conceal large gross underlying positions that can give rise to significant concentration risk.

Adequate market risk management practices vary widely across financial institutions depending on the nature, complexity and diversity of their market activities. Financial institutions should have robust governance arrangements, including a clear organizational structure with well-defined, transparent and consistent lines of responsibility and effective processes to identify, measure, manage, monitor and report the risk they are or might be exposed to.

5.2 Organization Structure

a) Effective Board and Senior Management oversight is a key to managing overall market risk exposure of financial institutions. The BODs, in this regard, should fulfill the following responsibilities:

   i) Approve risk appetite and risk tolerance in relation to market risk and periodically assess and update the risk appetite and tolerance level.

   ii) Ensure overall market risk exposure is within appropriate limits and consistent with the available capital.

   iii) Ensure that top management as well as senior executives responsible for market risk management have sound knowledge, expertise, and experience to fulfill risk management functions.

   iv) Ensure development and implementation of clear, effective, and sound market risk management principles, facilitating the identification, measurement, monitoring, and control of market risks.

   v) Ensure sufficiency of financial, technical, human, and physical resources to ensure sound market risk management within the institution.

b) The senior management should be responsible to implement guidelines, policies, processes, and procedures, in line with the strategic directions and goals set by the BODs for the management of market risk. More specifically, senior management is responsible to:

   i) Develop, implement, and update processes and procedures that translate the strategic intent or goals of the BOD into clear, transparent, and comprehensive operating standards.

   ii) Ensure due consideration to established lines of authority and responsibility for measuring, identifying, managing, and reporting market risk.

   iii) Plan the use of information technology to identify, measure, monitor, and control financial institution's market risk. Such technology should also support early warning signals to control worsening situations.

   iv) Establish and implement effective internal controls to monitor and control market risks.

   v) Implement market risk management policies, approved by the BODs.

c) The organization of the market risk management varies depending on the nature, size and scope of business activities of the financial institution. It should be aligned with the risk profile of the financial institution and the overall risk strategy set by the board, with clear lines of authority. The risk-taker units should be aware of the organization’s risk profile, products and limits assigned to them. The market risk management function should be independent with clear reporting lines. For proper management of market risk, financial institutions should set up committees at various level including a Risk Management Committee, and Asset-Liability Management Committee (ALCO).

d) The Risk Management Committee (RMC) involves board members and supervises overall risk management functions of the financial institution. The RMC should ensure that the bank has complete, clear, comprehensive, well-documented policies and procedural guidelines regarding

the management of market risk. Policies and procedural guidelines should be approved by the board and after that disseminate for implementation. It must assess the strength of management information system for adequate risk reporting and ensure robustness of financials models in the management of market risk.

e) The Asset-Liability Management Committee (ALCO) is responsible for the supervision/management of Market Risk. It may monitor maturity mismatch, gap identification, market risk inherent to new products, structure and composition of the financial institution's assets.

f) The first line of risk management functions in the business units (i.e. Middle office), where market risk arises, monitors, measures, and analyzes risks inherent to market operations and prepares reports for senior management and ALCO. Depending on the size, complexity and diversity of their activities, financial institutions must select various methods and methodologies, ranging from simple gap analysis to computerized modeling techniques.

5.3 Strategy Policies, and Procedures

a) Based on its risk profile and the level of market risk it is willing and/or able to take, the financial institution should develop a strategy to manage its market risk. The market risk management strategy should be aligned with the institution's objectives, risk appetite and risk tolerance. Approved by the board, the market risk management strategy should be well communicated within the financial institution. The market risk strategy should be periodically updated (at least once a year and immediately in case of change in market activity), and regularly reviewed to accommodate changes in business/strategic plan and significant developments in the external operational environment.

b) Policies and procedures should clearly define and describe risk management tools that the financial institution plans to use to effectively identify, measure, manage, monitor and report the market risk to which it is exposed. The various steps should be documented and communicated throughout the organization.

c) Policies should include clear definitions of roles and responsibilities of individuals and teams performing market risk management functions, including structural balance sheet management, pricing, marketing, management reporting, lines of authority and responsibility for market related decisions.

d) Specific policies and procedures should be put in place for new products and activities.

e) Financial institution should implement stress testing to measure system resilience.

5.4 Limits and indicators

a) An important dimension of the market risk management framework is the quantification of market risk which the financial institution faces, taking into account the institution's current portfolio and a forward-looking perspective based on budget figures as well as on behavioral approaches of on- and off-balance sheet items that can broadly differ with the contractual approach.

b) To control its market risk exposure and vulnerabilities, a financial institution should set limits. The limit system should be established, taking into account the institution's risk appetite, in order to mitigate market risk, taking due account of risk concentrations.

c) Financial institutions must set limits based on portfolio, type of activity, product and strategy. Risk- taking units must have procedures for activities, which aid risk-takers to understand their limits and to ensure they operate within the approved limits. Limit breaches should be immediately escalated to senior management as and when they occur.

d) Different sets of limits should be put in place to cover intraday and overnight exposures. While assessing how limits would perform under stressed conditions, a financial institution should include measures aimed at ensuring that it can continue to operate in a period of market stress, institution-specific stress and/or a combination of two.

e) Common approaches to measuring and limiting market risk are:

   i) Formulate detailed structure of market risk limits that are consistent with the institution's risk appetite, risk profile and capital strength,

   ii) Set limit on open positions in each type of product, limit may be based on nominal size or /and percentage of position,

   iii) Set limit on concentration and identify areas of diversification of investment,

   iv) Use appropriate quantitative techniques, such as Value-at-Risk, to identify and measure market risk.

f) In addition, financial institutions should design a set of indicators to identify the emergence of increased risk or vulnerabilities in their market exposures.

5.5 Measurement and Monitoring

a) Measuring market risk is crucial for estimating potential losses to the financial institutions in event of any loss. It also helps them to ensure that potential losses resulting from market risk fall within their risk appetite and would not substantially erode capital and earnings.

b) Financial institutions should ensure they have in place appropriate management information system (MIS) for accurate and timely identification, aggregation, monitoring, controlling, and reporting of market risk and aid it developing market risk reports to board and senior management.

c) Financial institutions should monitor their market risk by using different techniques and models. They should ensure that at any time their exposures fall within their market risk tolerance. To strengthen the monitoring, financial institutions may conduct stress testing to assess the vulnerability of their strategies and positions. The selection of stress test scenarios must suit the size, complexity and diversity of activities. While considering stress test, emphasis should be placed on concentration of instruments and markets, when positions are difficult to liquidate under stressful situations.

d) Internal audit plays a vital role in the monitoring and control of market risk by reviewing and validating the market risk measurement process regularly; it also contributes to ensuring the accuracy of data entered in risk models, validity of risk models and risk measurement calculations, reasonableness of scenarios and assumptions.

5.6 Control of market risk

a) To reduce their market risk exposure, financial institutions should ensure adequate training and segregation of duties among front, middle and back office.

b) The financial institution's management information system should generate periodic reports that depict the actual size, return, risk, potential profit or loss etc. of the exposure and such report should be forwarded to board and senior management for review

c) Financial institutions should have adequate internal controls to ensure proper risk management process. These internal controls should be an integral part of the institution's overall risk management system. They should promote effective and efficient operations, reliable financial and regulatory reporting, and compliance with regulatory requirements.

d) Appropriate contingency plans should be put in place.

VI – Management of Interest Rate Risk in Banking Book

6.1 Overview

Interest Rate Risk in the Banking Book (IRRBB) refers to the current or potential risk to a bank's capital and earnings arising from adverse movements in interest rates that impact banking book positions. Such changes affect not only the earnings of a bank but also the underlying economic value of its assets, liabilities, and off-balance sheet items. IRRBB can pose significant threats to both the current capital base and future profitability of financial institutions. IRRBB typically encompasses the following types of risks:

a) Repricing risk, arising from mismatches in the timing of interest rate resets on assets, liabilities, and off-balance sheet positions.

b) Yield curve risk, which emerges from changes in the slope or shape of the yield curve, even when repricing dates match.

c) Basis risk, resulting from imperfect correlation between different interest rate indices used for pricing instruments with similar repricing characteristics.

d) Optionality risk, which comes from embedded options in banking products (e.g., loan prepayments, early deposit withdrawals), whose value can fluctuate with interest rate movements.

Assessment of IRRBB requires two complementary perspectives:

a) The earnings perspective, which focuses on how changes in interest rates affect a bank's short-term net interest income (NII).

b) The economic value perspective, which evaluates the impact of interest rate movements on the present value of future cash flows of assets, liabilities, and off-balance sheet items - offering a longer-term view of risk.

Banks are expected to establish robust governance arrangements to manage IRRBB effectively. This includes a clear organizational structure with defined lines of responsibility, comprehensive risk identification and assessment procedures, and systems to monitor, control, and report interest rate risk exposures. Institutions should also have sound internal control mechanisms and risk management practices to manage IRRBB as part of their overall risk governance framework.

6.2 Organization Structure

a) The organization of the interest rate risk management depends on the nature, size and scope of activities of the financial institution, the complexity and nature of its business, as well as the level of interest rate risk exposure.

b) Risk management function should be engaged in monitoring interest rate risk levels, setting out interest rate risk indicators, timely and accurate reporting of important interest rate risk related information, and the development of interest rate risk management policies. The head of this function should directly report to the CRO.

c) Financial institutions should clearly define the individuals and/or committees responsible for managing interest rate risk and should ensure that there is adequate separation of duties in key elements of the risk management process to avoid potential conflicts of interest.

d) Depending on the size, risk exposure, and diversity of activities, financial institutions may establish an ALCO to oversee the management of interest rate risks as well as the financial institution's funding, balance sheet management etc.

e) An appropriate MIS should be implemented to identify, measure, monitor, control and report interest rate risk. The reports should be forwarded to senior management and the board.

6.3 Strategies, Policies and Procedures

a) Financial institutions must have appropriate strategies, policies and procedures in place to perform effective interest rate risk management that maintains such risk within prudent levels which is essential for the safety and soundness of the institution.

b) IRRBB strategy should reflect a proper alignment between interest rate risk profile and business plans and should have proper risk management system in place. IRRBB strategy should take into account composition, tenure and diversification of loans, deposit and investment as such risk has a significant impact on profitability and capital.

c) IRRBB policies and procedures should be incorporated into ICAAP.

d) IRRBB policy should be clearly defined and consistent with the nature and sophistication of their activities, with a clear set of institutional procedures for acquiring specific instruments, managing portfolios, and controlling the total interest rate risk exposure. Further, all interest rate risk policies should include specific procedures and approvals necessary for exceptions to policies. They should be reviewed periodically and revised as needed.

6.4 Limits

a) The management must establish prudent limits to ensure that the bank's interest rate risk exposure remains within the Board approved risk tolerances across a range of potential interest rate scenarios.

b) These appetite limits should be approved by the board; however, the board of directors or a designated committee should periodically review their appropriateness to ensure continued alignment with the bank's overall risk appetite and market conditions.

c) Keeping in view the size, sophistication, nature of operations and underlying risks; limits should be further specified for certain types of instruments, portfolios, and activities. Also, specific procedures and approvals necessary for exceptions to limits, and authorizations should be specified.

6.5 Risk Measurement

a) Financial institutions should set up appropriate IRRBB measurement systems that capture all material sources of IRRBB and that assesses the effect of interest rate changes consistent with the scope of their activities. In measuring interest rate risk, financial institution can consider repricing risk, yield curve risk, basis risk, optionality risks, fee-based and any other income sensitive to changes in interest rates.

b) The assumptions underlying the system should be reasonable and clearly understood by those engaged in the management of IRRBB. Financial institutions must have an integrated view of such interest rate risk across activities, products and business lines.

c) Risk measurement systems should evaluate concentrations of positions taken and ensure interest-sensitive positions are commensurate with the complexity and risk inherent in those positions.

Financial institutions may employ quantitative techniques to measure and manage IRRBB including:

i) Gap Analysis, which identifies mismatches in the timing of rate changes between assets and liabilities;

ii) Earnings-at-Risk (EaR), which measures the potential short-term impact on net interest income due to rate shocks;

iii) Economic Value of Equity (EVE), which assesses the long-term impact of interest rate changes on the present value of future cash flows;

iv) Duration Analysis, that estimates the sensitivity of the economic value of assets and liabilities to interest rate changes;

v) Stress Testing, that simulates scenarios to assess vulnerability to losses under stressful market conditions, taking into consideration institution's risk profile to gauge its resilience.

d) These tools shall complement regulatory provisions and provide a comprehensive understanding of interest rate risk exposures. Results from stress testing and such quantitative techniques should be considered when reviewing their policies and limits for interest rate risk in banking book.

e) All models and techniques used for IRRBB measurement and reporting should be subject to independent validation and periodic review to ensure their accuracy, relevance, and effectiveness under evolving market conditions.

6.6. Risk Monitoring and Reporting

a) An accurate, informative and timely management information system (MIS) is essential for managing interest rate risk exposure, both to inform the management and to support compliance with the board approved policy.

b) Keeping in view the size, sophistication and nature of operations and underlying risks, a financial institution should have adequate mechanism for monitoring and reporting interest rate risk that adequately covers all material risks. The reporting system should be clearly documented providing formats and frequency of the reports for the board or its subcommittee and different hierarchical levels of the management. These reports should, but not limit to:

i) convey the magnitude, sources and trends of the bank's aggregated interest rate risk exposures;

ii) demonstrate the bank's compliance with policies and limits;

iii) the reasonableness of key assumptions and parameters for movement in the interest rate risk;

iv) results of stress tests; and

v) summaries of the findings of reviews of interest rate risk policies, procedures and the adequacy of the interest rate risk measurement systems, including any findings of internal and external auditors.

6.7 Internal Control

a) Adequate system of internal controls should be placed requiring regular independent reviews and evaluations of the effectiveness of the interest rate risk management process with appropriate revisions or enhancements to internal controls. These internal controls should be an integral part of the institution's overall system of internal control and be consistent with regulatory requirement and policies of the financial institution.

VII – Technology Risk Management

7.1 Overview

Technology plays a crucial role in commercial banking, enabling digital banking, online transactions, data management, and cybersecurity. However, reliance on technology also introduces significant risks such as cyber threats, system failures, fraud, data breaches, and regulatory non-compliance. These guidelines aim to strengthen system resilience, ensure robust cybersecurity practices, protect customer data and enhance customer trust.

7.2 Organization Structure

Financial institutions should establish a robust governance structure to ensure accountability and oversight of technology risk management, which includes:

a) The BOD should oversee the development and approval of an IT risk management framework. Additionally, the Board should ensure compliance with central bank directives and international security standards while allocating adequate budget and resources for cybersecurity initiatives.

b) Risk Management Committee (RMC) or Committee delegated by Board should monitor IT risk exposure, review technology risk reports and recommend mitigation strategies.

c) Chief Information Officer (CIO) / Chief Technology Officer (CTO) should oversee IT infrastructure, software, and cybersecurity systems. Further, the Chief Information Security Officer (CISO) should develop and enforce IT security policies to ensure robust risk management, oversee cyber threat detection and response mechanisms and ensure compliance with regulatory and industry cybersecurity frameworks.

d) Technology Risk Management Team should conduct risk assessments, penetration testing and system audits, and monitor security alerts and manage cybersecurity incidents.

e) The Internal Audit and Compliance Team should ensure the bank follows central bank regulatory provisions on Information System Audit (IS Audit) and cybersecurity.

7.3 Strategies, Policies and Procedures

a) Financial institutions should have sound Technology Risk Management Strategy which should align TRM with business objectives, regulatory requirements, and international cybersecurity standards (e.g., ISO/IEC 27001, Basel guidelines), implement a risk-based approach for IT security and operational resilience, and establish a cybersecurity culture through training and awareness programs.

b) Key IT Policies should include access control policy, data protection policy, incident response policy, third-party risk management policy, etc.in line with NRB Information Technology Guidelines, 2012.

c) These policies and procedures should describe technology change management, data backup and recovery, and user training and awareness to ensure secure, reliable, and efficient operation of the financial institution’s IT systems.

d) A comprehensive Digital Fraud Prevention Policy should be in place that entails digital fraud risk controls such as governance and oversight of digital frauds, customer dispute handling system and appropriate operational controls to protect the customers from digital banking frauds and enhance customers' trust in the financial sector.

e) A robust cyber security management framework in alignment with NRB Cyber Resilience Guidelines, 2023 should be in place that incorporates cyber security risk identification, risk rating system for categorization of cyber security vulnerabilities and prioritization of critical information assets, cyber security incident response plan, security testing, timely risk reporting and cyber threat intelligence to identify and manage potential cyber threats from all sources to strengthen cyber security system in the institution.

f) Financial institutions must ensure ethical and responsible use of futuristic technologies such as Artificial Intelligence (AI) and Machine Learning in the institution and identify and mitigate potential additional risk exposures associated with them.

7.4 Risk Identification, Assessment and Measurement

a) The identification of key technology risks should include, at a minimum, cybersecurity threats, data breaches, system failures, fraud and identity theft, third-party risks, and regulatory non-compliance.

b) Financial institution should use risk assessment matrices to evaluate risks based on its likelihood and impact, conduct penetration testing and ethical hacking to assess system vulnerabilities, and implement scenario analysis and stress testing to measure system resilience.

7.5 Monitoring and Reporting

a) Senior management should ensure a process for continuous monitoring to deploy real-time security monitoring systems (SIEM, firewalls, intrusion detection systems), conduct regular vulnerability assessments and security audits and implement automated fraud detection systems to identify suspicious transactions.

b) Technology Risk Management requires incident reporting mechanisms to establish a Cybersecurity Operations Center (SOC) for real-time threat monitoring, implement a clear escalation process for reporting IT security incidents, and conduct post-incident reviews to improve security measures.

c) These risk reports may contain Key Risk Indicators (KRIs) and Metrics that are relevant for decision making.

7.6 Contingency Planning and Business Continuity Management

a) It should include IT Disaster Recovery Plan (DRP) which maintains backup data centers with redundant systems, implement automated data backups and test recovery processes regularly, and define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical banking services.

b) It should include Cyber Incident Response Plan, establish a dedicated Cybersecurity Incident Response Team (CIRT), implement isolation protocols to contain cyberattacks, and conduct forensic investigations to identify attack sources and mitigate future risks.

c) Financial institutions should develop Business Continuity Planning (BCP) strategies to maintain critical operations during disruptions and ensure the availability of backup systems and processes for swift recovery, ensure test of BCP and DRP periodically to validate their effectiveness.

VIII – Climate Risk Management

8.1 Overview

Climate change and extreme weather changes continue to affect millions of people, inflicting devastating consequences such as causing loss in lives, livelihood and damage to physical structure, among others. Given their likelihood, unpredictable nature, considerable impact and potential to be a systemic risk, they pose a real threat to global financial stability.

Generally, climate related risks can take two forms: physical risks, arising from extreme weather events, long term gradual shifts of the climate or indirect effect of climate change and transition risks, arising from the process of transitioning to a low carbon economy[1]. Both of these risks could adversely impact the soundness of financial institutions and stability of the financial system. The guidelines on climate risk management set out the supervisory expectations for banks and financial institutions related to their approach in identifying, addressing and mitigating climate and environment related risks and their impacts in the financial sector and aim to strengthen resilience against such exposures while integrating these risks into the existing risk management framework.

8.2 Organization Structure

a) The Board of directors (BOD) should consider climate related risks while preparing the goal, business strategy and overall risk strategy of the financial institution. The board should be responsible for the effective oversight of such risks within the institution.

b) The board is expected to have a sound understanding of the climate related risk exposure taken by the institution as well as the potential risks that could materialize over various time horizons and must develop robust processes for the management of such risks.

c) Climate related risks should be embedded in the risk management framework and the Board should monitor, on an ongoing basis, the climate related extreme events and its impact on the business activities. Financial institutions must duly follow the ESRM Guidelines for Banks and Financial Institutions, 2022 in order to integrate Environmental & Social risk management into the overall credit risk management process.

d) The climate related financial risks should be addressed in the institution's risk appetite framework. Climate related responsibilities and reporting lines must be clearly assigned across the three lines of defense in the institution.

e) The Senior Management should assign clear lines of responsibility and authority to the management level positions or related committees for the management of climate related risks to ensure prompt response and accountability.

f) The Senior Management should ensure effective implementation of the strategic plan and processes that addresses the climate related risks within the business functions.

[1] Climate-related risk drivers and their transmission channels (April 2021), Basel Committee on Banking Supervision

g) Financial institutions should ensure Climate risk related strategy is aligned with its business strategy and business objectives in the Risk Management Framework.

8.3 Strategies, Policies and Procedures

a) The Board should formulate climate-related strategies and policies that adequately addresses the impact of climate-related financial risks on the financial institutions' credit risk, market risk, liquidity risk, operational risk, and other types of risks.

b) A climate risk committee should be formed, meeting on a quarterly basis, to formulate guidelines on climate risk management, and advise the board on the matters relating to climate and environment related risks.

c) Financial institutions should develop strategy for required investment in resilient infrastructure such as flood defenses, reinforced structures, and energy-efficient buildings to enhance the durability of physical assets, reduce potential damage, and lower long-term operational costs.

d) Financial institutions should proactively strengthen asset resilience and incorporate these insights into risk management for mitigating potential losses, supporting business continuity, and aligning with evolving regulatory and sustainability expectations.

e) Awareness programs/activities on climate exposure risks should be conducted periodically within its institution as well as with the related stakeholders.

f) The financial institutions should focus on developing risk awareness culture and continuously build their capabilities and expertise on climate-related and environmental risk management in line with the international standards and developments and the climate and environment related risks and events they are exposed to.

8.4 Risk Identification, Assessment and Measurement

a) Financial institutions should aim to identify, assess, and measure climate related physical and transition risks within the financial system. Banks should understand and evaluate their exposure to sectors and activities that may be affected by climate-related factors, including agriculture, infrastructure, energy, and other environmentally sensitive sectors.

b) To effectively manage climate-related risks to physical assets, banks are encouraged to conduct comprehensive climate vulnerability assessments that evaluate exposure to hazards such as floods, landslides, etc. These assessments help identify high-risk assets and support the development of targeted mitigation strategies.

c) The institution may, on an annual basis, conduct scenario analysis and stress testing exercises in short term, medium term and long-term period and assess resilience of the system against such impacts.

d) Stress testing can make use of both bottom up and top-down approach to measure the impact of such risks to the institution. It should consider limited data availability, limited technical capabilities, impact of various assumptions on the test models and it should be updated frequently based on the policy developments and regulatory directions on climate and environment related risks.

e) For example, scenario analysis could consider a certain most significant climate hazard (landslide/draught/flood), focus on a certain most vulnerable geographical region (geographic susceptibility to extreme weather) or focus on a specific risk category (losses in credit portfolio due to extreme climate events or natural disasters).

f) The results of the stress test exercises may be incorporated in formulation of climate and environment related guidelines based on results.

8.5 Internal Control

a) The board should ensure internal controls in place for the identification, categorization, management and mitigation of climate related financial risks.

8.6 Monitoring and Reporting

a) Financial Institutions are encouraged to establish robust systems for ongoing monitoring and reporting of climate risk exposures and mitigation measures. These systems should be flexible and adaptive, allowing for the capture of emerging risks, integration of new data, and responsiveness to evolving regulatory and environmental conditions.

b) While measuring and monitoring the impact of climate and environment related risk on the business activities and policies, the climate related risk reports may contain Key Risk Indicators (KRIs) and Metrics related to both physical and transition risks that are relevant for decision making.

c) This risk report may include monitoring exposure to climate-vulnerable sectors, assessing the progress of adaptation or resilience investments, and evaluating emissions intensity along with other relevant sustainability metrics.

d) Internal reporting frameworks should ensure timely and transparent communication of climate risks, provide regular updates on mitigation efforts, and effectively deliver relevant information to senior management and oversight committees for informed decision-making.

e) Financial Institutions may align climate reporting with frameworks like ISSB and GRI for consistency. Regular review and validation of data and methods are essential to ensure accurate and relevant climate risk reporting.

8.7 Contingency Planning

a) Financial Institutions should develop contingency plans that address potential disruptions from both physical and transition-related climate risks, including clear protocols for extreme weather/climate events to ensure operational continuity under adverse climate conditions.

b) These contingency measures must be integrated within the broader risk management frameworks and aligned with monitoring and reporting systems to enable timely detection, effective communication, and rapid response to emerging climate risks.

c) Regular testing and update of contingency plans are essential to reflect evolving climate risks, emerging data, and lessons learned from actual events or simulation exercises.

***

Annexure

Annexure 1: Sample Template - Risk Appetite and Risk Tolerance

A. Credit Risk

S.N.	Particulars	Regulatory Requirement	Risk Appetite	Risk Tolerance	Frequency	Responsible Unit	Escalation/ Action
1	Non-performing Loan						
2	SOL Exposure Limit						

B. Technology Risk

S.N.	Particulars	Regulatory Requirement	Risk Appetite	Risk Tolerance	Frequency	Responsible Unit	Escalation/ Action
1	Mobile Banking Downtime						
2	Recovery Time Objective (RTO)						

Note: Banks and Financial Institutions are required to set their Risk Appetite and Risk Tolerance limits for all risks mentioned in this guideline.