Website: www.bb.org.bd

Department of Off-Site Supervision
Bangladesh Bank
Head Office
Dhaka

DOS Circular No. 04 **Date: 8 October, 2018 / 23 Ashwin , 1425**

Chief Executives
All Scheduled Banks in Bangladesh

Dear Sir,

Risk Management Guidelines for banks

Please refer to DOS circular no.02 dated February 15, 2012 and DOS circular letter no.13 dated September 9, 2015 on the captioned subject.

Bangladesh Bank (BB) has continued its effort for upgrading the initiatives taken to manage various risks of banks in a prudent manner. Meanwhile, core risk management guidelines and other risk related guidelines have been revised. Moreover, modification of the prudential regulations is done on regular basis. As part of this endeavor, the previous guideline has been revised for ensuring sound risk management culture effectively in the banks and all scheduled banks are hereby instructed to follow the attached 'Risk Management Guidelines for Banks'. Each bank shall prepare a comprehensive risk management guideline following this latest one and considering its nature, size and complexities of business activities, get it approved by the board and shall submit a copy to the Department of Off-site Supervision (DOS) for information. The bank shall review the guideline at least once a year for adapting with the changing environment. Besides, banks shall reconstruct its risk management organogram and appoint Chief Risk Officer (CRO) as the head of Risk Management Department (RMD) following the instructions of the revised risk management guidelines issued by BB. For ensuring proper identification, measurement, timely treatment of risks and implementation of the said guideline, the banks are also instructed to submit the following reports to DOS of BB within the stipulated time frame :-

1. Soft copies of risk management reports (CRMR prepared for June & December and MRMR for all other months) for successive months of each quarter along with the minutes of monthly Executive Risk Management Committee (ERMC) meeting within the next month of the reporting quarter;
2. Board Risk Management Committee(BRMC) meeting minutes within 7 days of the meeting held;
3. Board approved Risk Appetite Statement (RAS) on yearly basis within first two months of the year;
4. A soft copy of Stress Test report on half yearly basis along with CRMR;
5. A review report of Risk Management Policies and effectiveness of risk management functions with the approval of the board of directors by the end of 2nd month following the end of each year.

Instructions of DOS circular No.02 dated February 15, 2012 and DOS circular letter no.13 dated September 9, 2015 hereby stand superseded by this circular.

This circular along with the guidelines are available on the website of Bangladesh Bank and shall come into force with immediate effect.

Yours sincerely,

Enclosure: As above

Sd./-

(Md. Sirajul Islam)
General Manager (Current charge)
Phone: 9530081

Risk Management Guidelines for Banks

October 2018

Department of Off-site Supervision
Bangladesh Bank

Preamble

Taking risk is an integral part of financial intermediation and banking business. Failure to assess and manage risks adequately may lead to losses endangering the soundness of individual financial institutions and affecting the stability of the overall financial system.

The banking sector throughout the world underwent a vulnerable situation due to recent global financial crisis. Developing countries like Bangladesh were also affected in the aftermath of the global financial crisis. Consequently, poverty and human inequality increased significantly around the world as well as the indicators of human resources development also deteriorated. Weak risk management, though cannot be considered as a specific trigger for the financial crisis, has been identified along with weak internal governance as an underlying factor. Where they existed, sound risk management practices helped institutions to endure financial crisis significantly better than others.

Relationship between our local banks and internationally recognized banks has expanded due to increase in foreign trade and commerce. The competition among the banks has increased and new and complex products/services/technology platform have been introduced. As a result, risk in the banking industry has increased remarkably as compared to that of earlier time. It is indispensable to ensure risk management culture/practice at enterprise level to conduct business successfully with the internationally renowned banks, to upgrade the banks' financial soundness indicators to a satisfactory level, and over all, to maintain financial stability in the banking sector.

The setting of an appropriate strategy and risk tolerance/appetite levels, a holistic risk management approach and effective reporting lines to the competent authority in its management and supervisory functions, enables management of banks to take risks knowingly and treat risks where appropriate. Risk management is a part of internal governance involving all areas of banks. There is a strong link between good corporate governance and sound risk management. Without proper risk management, the various functions in a banking institution cannot work together to achieve the bank's objectives. It is an essential part of helping the bank to grow and promote sustainability and resilience.

There is no alternative but to ensure sound risk management practices for surviving in the competitive environment. Therefore, banks should give greater emphasis on continuous improvement in risk management, and set their performance goals in line with strategic planning/objectives. While the extent of risk management function performed and structure kept in place depend on the size and complexity of individual banks, risk management is most effective when basic principles and elements of risk management are applied consistently throughout the financial institution.

Risk management is a discipline at the core of every enterprise and encompasses all activities that affect its risk profile. However, this function needs not be uniform across all banks. The definition of a sound or adequate risk management system is ever changing, as new technology accommodates innovation and better information and as market efficiency grows. Each banking institution should put in place a comprehensive risk management program tailored to its needs and the circumstances under which it operates. In this context, BB has revised previously issued six (06) core risks guidelines to adapt with the changing banking environment as well as to deal with various risk issues prudently. Yet risk management in banks should further move from a compliance-driven function toward a top level comprehensive activity relevant at the highest levels of decision making and strategy setting.

Chief Advisor

S. M. Moniruzzaman
Deputy Governor
Bangladesh Bank

Advisor

S. M. Rabiul Hassan
Executive Director
Bangladesh Bank

Coordinator

Md. Arifuzzaman
Deputy General Manager
Bangladesh Bank

Members of Working Committee

Md. Aminur Rahman Chowdhury, Joint Director, Bangladesh Bank
A. N. M. Moinul Kabir, Joint Director, Bangladesh Bank
Jebunnessa Karima, Joint Director, Bangladesh Bank
Mohammad Atiqur Rahaman, Deputy Director, Bangladesh Bank
Shirajum Munira, Deputy Director, Bangladesh Bank
Md. Jahangir Alam, EVP, AB Bank Ltd.
Md. Ashraful Azim, SVP, Shahjalal Islami Bank Ltd.
Pronob Kumar Roy, SAVP, Dutch Bangla Bank Ltd.
Md. Nurul Huda, AGM, Agrani Bank Ltd.
M. Shahed Wali, Sr. Credit Manager, Standard Chartered Bank

Table of Contents

List of Acronyms

ADR	Advance Deposit Ratio
ALCO	Asset-Liability Management Committee
ALM	Asset Liability Management
BB	Bangladesh Bank
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
BOD	Board of Directors
BIU	Basel Implementation Unit
BRMC	Board Risk Management Committee
CCD	Central Compliance Department
CRAR	Capital to Risk Weighted Asset Ratio
BCP	Basel Core Principles
CRO	Chief Risk Officer
CRR	Cash Reserve Ratio
ERMC	Executive Risk Management Committee
ICAAP	Internal Capital Adequacy Assessment Process
MCO	Maximum Cumulative Outflow
MIS	Management Information System
OBS	Off-Balance Sheet
RAF	Risk Appetite Framework
RAS	Risk Appetite Statement
RMD	Risk Management Division/Department
RWA	Risk Weighted Asset
SLEPT	Socio-cultural, Legal, Economic, Political and Technological analysis
SLR	Statutory Liquidity Requirement
SLP	Structural Liquidity Profile
SWOT	Strengths, Weaknesses, Opportunities & Threats analysis
VaR	Value at Risk
WBG	Wholesale Borrowing Guidelines

Chapter 1

Objective of Risk Management

1.1 Introduction

This guideline is issued by Bangladesh Bank (BB) under section 45 of the Bank Company Ain, 1991 with a view to providing a structured way of identifying and analyzing potential risks, and devising and implementing responses appropriate to their impact. These responses generally draw on strategies of risk prevention, risk transfer, impact mitigation or risk acceptance.

This guideline is prepared in line with internationally accepted risk management principles and best practices. The guideline is also aligned with the revised version of Basel Core Principles (BCP) for Effective Banking Supervision published by the Basel Committee on Banking Supervision (BCBS) in September 2012. The BCP on 'Risk Management Processes' (CP15) requires that banks have a comprehensive risk management process (including effective board and senior management oversight) to identify, measure, evaluate, monitor, report and control or mitigate all material risks on a timely basis and to assess the adequacy of their capital and liquidity in relation to their risk profile and market and macroeconomic conditions. The risk management process is commensurate with the risk profile and systemic importance of the bank. Other relevant CPs touch on Corporate Governance (CP14), Capital Adequacy (CP16), Credit Risk (CP17), Problem Assets Provisions and Reserves (CP18), Concentration Risk and Large Exposure Limits (CP19), Market Risk (CP22), Liquidity Risk (CP24), Operational Risk (CP25), Interest Rate Risk (CP23), Financial Reporting and External Audit (CP27), Disclosure and Transparency (CP28).

1.2 Scope of Application

The guideline pertains to all scheduled banks (conventional, islamic shariah and islamic banking branches/windows of conventional banks) operating in Bangladesh.

In issuing the guidelines, Bangladesh Bank intends to provide guidance to all banks on minimum standards for risk management. These Guidelines are not intended to be so comprehensive as to cover each aspect of a bank's risk management activity. A bank may, depending on its size and complexity, establish a more sophisticated framework than outlined in this document.

However, Bangladesh Bank considers compulsory for all banks to self-assess their risk profile and operational context, and customize their risk management architecture and approach to attain organizational goals while meeting the minimum requirements set out in the guidelines.

1.3 Objectives

In publishing the guidelines, the objectives of Bangladesh Bank are:

- To promote better risk culture at all levels of the banks.
- To provide minimum standards for risk management practices.
- To improve financial soundness of individual banks and stability of the overall financial sector.
- To encourage banks to adopt and implement a sound risk management framework.
- To introduce important risk management tools and techniques for assessment and necessary treatment of various risks.

1.4 Dimensions of Risk Management

1.4.1 Risk Culture

Every banking 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 banks 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.

A bank should develop its risk culture through policies, examples, communication, and training of staff regarding their responsibilities for risk. Every member of the bank should be fully aware of his or her responsibility regarding risk management. Risk management should not be confined to risk specialists or to control functions. Business and operational units, under the oversight of the management body, should be primarily responsible for managing risk on day-to-day basis, considering risk tolerance and risk appetite, and in line with bank'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 risk culture are often the root cause for occurrence of significant risk events, financial institution failures, and financial crisis.

The top level of the bank sets the tone for the desired risk culture. The risk culture can be strengthened through:

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

- Clarifying the range of acceptable risks using an embedded risk appetite statement and various forms of communication and training; and,
- Aligning incentives with objectives and clarifying how breaches in policies/procedures will be addressed.

1.4.2 Risk Strategy and Risk Appetite

Risk tolerance and risk appetite are terms often used interchangeably: risk appetite describes the absolute risks a bank is a priori open to take; while risk tolerance relates to the actual limits that a bank has set.

A bank'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 bank should have risk goals and risk strategies which enable them to achieve the desired risk profile.

The board of directors sets the strategies and the senior management is responsible for implementing those strategies and communicating them throughout the organization.

Risk appetite statement plays an important role in cascading the risk strategy down through the institution. It should include metrics and indicators in relation to specific risk types. The risk-appetite statement should be well-embedded and be consistent with the bank's capacity to take risk, taking into consideration the capital constraints, and potential profit and loss consequences.

A good practice includes the followings:

- Regular review of risk appetite statement as a formal process;
- Top-down and bottom-up processes to define risk metrics and risk appetite; and,
- Limit systems that are aligned with overall governance so that breaches are quickly flagged and appropriate counter-measures are taken.

1.4.3 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 the ways the board influences risk-related decisions; and the role, structure, and staffing of risk organization. A good practice in this dimension is where the board has regular involvement in managing key risk issues, and risk management responsibilities are proportionate to the risks assumed at a particular level or unit.

Risk governance should follow a three-lines-of-defense-model.

The first line of defense provides that the business and operation units of the institution have in place effective processes 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 followings:

- adequate control of risks;
- prudent conduct of business;
- reliability of financial and non-financial information reported or disclosed (both internally and externally); and,
- compliance with laws, regulations, supervisory requirements, and the institution's internal policies and procedures.

The Internal Control framework encompasses 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, headed by a Chief Risk Officer, has the responsibility for recommending and monitoring the bank'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 bank's internal audit which performs independent periodic reviews of the first two lines of defense, provides assurance and informs strengths and potential weaknesses of the first two lines.

1.4.4 Risk Assessment and Treatment

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

Risk management process is the systematic application of management policies, procedures and practices to the assessment, treatment, controlling, and monitoring 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 types of structure kept in place or strategies formulated by the bank, the risk management process should include proper risk assessment and treatment as described below.

1.4.4.1 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 impacts, 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 put in place adequate tools and techniques to identify risk because unidentified risks at this stage will not be included in further analysis.

Risk analysis involves developing an understanding of the risk. It provides an input to 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 consequences of an unfavorable event and likelihood of such event occurring. 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, banks 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 attention of the competent authority promptly. Risk evaluation mainly involves comparing the level of risk found during the analysis process with the bank's risk appetite, risk tolerance level and regulatory limits. Based on this comparison, the need for appropriate treatment should be considered.

1.4.4.2 Risk Treatment

After the exposed risks are assessed, banks should choose the best option to eliminate or 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:

- Avoiding the risk by deciding not to start or continue the activity that gives rise to the risk.
- Accepting and retaining the risk by making informed decision and having plans for managing and funding the consequences of the risk if it occurs.

- Reducing the likelihood of the risk through staff training, changing procedures, or by reducing the impact through diversifying credit portfolio, setting up off-site data backup etc.
- 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 banks 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 knowing when the risk becomes unacceptable and aligning their actions and behaviors with the institution's set risk appetite, risk tolerance, and strategy.

Monitoring and reviewing 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 risk management process for the purposes of:

- detection of changing risk sources and factors within and outside the institution,
- obtaining further information to improve risk assessment,
- ensuring that controls are effective and efficient in both design and operation,
- analyzing and learning lessons from events, trends etc., and
- identifying emerging risks.

Chapter 2

Risk Management System

A bank's risk management system shall include policies, procedures, limits, and controls in its foundation. 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 banks will depend on the effectiveness of the risk management system providing the foundation and arrangements that are put in place throughout the organization at all levels. The system 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.

2.1 Elements of a Sound Risk Management System

The key elements of a sound risk management system for effective business operations should encompass the followings:

a) Active involvement of board and senior management;
b) Adequate organization, policies and procedures;
c) Appropriate management information systems; and
d) Comprehensive internal controls and limits.

It should not be understood that risk management functions are only limited to the Risk Management Division/Department (RMD). Business lines are primarily responsible for the risks they are taking. Because the line personnel can understand the risks of their activities; any lack of accountability on their part may hinder sound and effective risk management.

2.2 Essential Criteria for Ensuring Sound Risk Management

For ensuring successful risk management across the organization, the following features should, at least, be present in the bank:

a) Submission of consolidated report to the board and senior management team incorporating different types of risks, risk mitigation measures, comparison of risk levels with limits, the level of capital required for absorbing large losses, and suggestions for restoring capital;
b) Consistency between the risks taken by the management and the risks perceived by the board;

c) Active, firm-wide risk management approach that includes all business lines;
d) Development of in-house expertise relying on various sources/factors including market data, credit ratings, published analyses, etc.;
e) Alignment of treasury functions with risk management;
f) Active management of contingent liabilities;
g) Use of both firm-specific and market-wide stress scenarios for liquidity management;
h) Efficient and effective management of asset and liability;
i) The stress testing result under consideration to understand the impact of adverse scenario on the bank's profitability or capital;
j) Independent risk management function with sufficient authority, logistic support and continuous communication with business lines;
k) Experienced and expert personnel for performing risk management activities;
l) Importance on the risk management officials' opinion.

2.3 Board and Senior Management Oversight

The top level authorities of the bank are responsible to ensure the ongoing effectiveness of the risk management system.

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. The senior management should be fully aware of the activities undertaken by the institution that could expose it to various risks. It should possess 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 bank's risk profile on an ongoing basis and should regularly report it to the board or a board level risk committee for review.

2.3.1 Board Oversight

The board of directors has the ultimate responsibility for the risks taken by the bank. Therefore, it must define the risk appetite, risk tolerance and risk limit, and set risk strategies. The board is responsible for understanding the nature of risks significant to the bank and for ensuring that the management is taking necessary steps to implement those strategies and manage accompanying risks.

To perform the risk oversight role properly, board members shall have a clear understanding of the types of risks inherent in business lines and take appropriate steps to ensure continued awareness of any changes in the level of risks. Board shall approve the strategies and significant risk management policies developed by senior executives and review them on regular basis. While performing their oversight function, board of directors should not be

involved in day-to-day activities of risk management. They shall make it clear to the bank's management that risk management is not an impediment to the conduct of business nor a mere supplement to a company's overall compliance program but is, instead, an integral component of the company's strategy, culture and value generation process.

2.3.2 Senior Management Oversight

While the overall responsibility for risk management rests with the board of directors, it is the responsibility of senior management to transform the strategic directions set by the board into operational policies, procedures, and processes for effective risk management. The senior management should be fully aware of the activities undertaken by the bank that could expose it to various risks. It should possess 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.

It has to ensure that the policies are embedded in the culture of the bank. It is also responsible for implementing risk management strategies and policies and ensuring that procedures are put in place to manage and control the risks in accordance with those policies keeping in view the strategic direction and risk appetite specified by board. For effective oversight of risk management, management shall provide the members of the board with sufficient information to enable them to understand the bank's risk profile, how risks are assessed and prioritized by the management team, risk response strategies, implementation of risk management procedures and infrastructure, and the strength and weaknesses of the overall system. To serve this purpose, management will oversee the development, implementation and maintenance of an appropriate Management Information System (MIS) that identify, measure, monitor and control bank's various risks. Through effective communications between the board and senior management, members of the board should be confident that the bank's executives understand the risks that the enterprise faces and are accomplished in their day-to-day management of enterprise risk.

2.4 Policies, Procedures and Limit Structure

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 bank's business and operational activities. The bank's policies and more detailed procedures should provide guidance for the day-to-day implementation of broad risk strategies, and generally should 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 the overall risk management.

The management should review risk policies, procedures, and limits in a timely manner and update them when necessary. Further, independent assurance from internal audit about the efficacy of these policies should also be obtained.

Banks shall consider the following key factors to ensure adequacy of policies, procedures and limits:

a) Proper documentation of policies, procedures and limits considering the risks associated with the activity, review and approval by the appropriate internal authority;
b) Assignment of full accountability and delegation of authority in the policies for each activity and product area; and
c) Development of compliance monitoring procedures incorporating internal compliance checks for adherence to all policies, procedures and limits by an independent function within a bank such as an internal control unit.

2.5 Risk Measurement, Monitoring and Management Reporting Systems

Banks shall perform the following key activities to ensure effective risk measurement, monitoring and management reporting systems:-

a) Identifying and measuring all quantifiable and material risk factors supported by proper information systems that provide the management with timely and accurate reports on the financial condition, operating performance and risk exposure of the bank.

b) Providing regular and sufficiently detailed reports (i.e. types of risk, impact on business, possible recommendations for mitigation etc.) on risk issues (if any) to line managers engaged in the day-to-day management of the bank's business operations.
c) Assessing the effectiveness of the risk measurement, monitoring and management reporting systems considering the adequacy of the risk monitoring practices and reports addressing all material risks; appropriateness of the key assumptions, data sources, procedures, analysis and documentation; adaption of changes in business or products; adequacy of information technology or management information system environment; consistency in management information reporting and other forms of communication; compliance with set limits, goals or objectives; adequacy, accuracy and timeliness of reports to the board and senior management.

2.6 Internal Controls and Comprehensive Audits

Internal control plays a critical role in managing risks of a financial institution. With 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, risk limit 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, limits on non-performing assets etc. These limits ensure that the bank's management does not take excessive risks while pursuing business targets.

The bank's internal control system should be adequately tested and reviewed by its internal audit. The coverage, procedures, and findings of the audit regarding the internal controls should be adequately reviewed by the Audit Committee and any material weakness found should be addressed promptly and appropriately.

Banks shall perform the following activities to ensure its internal control environment:

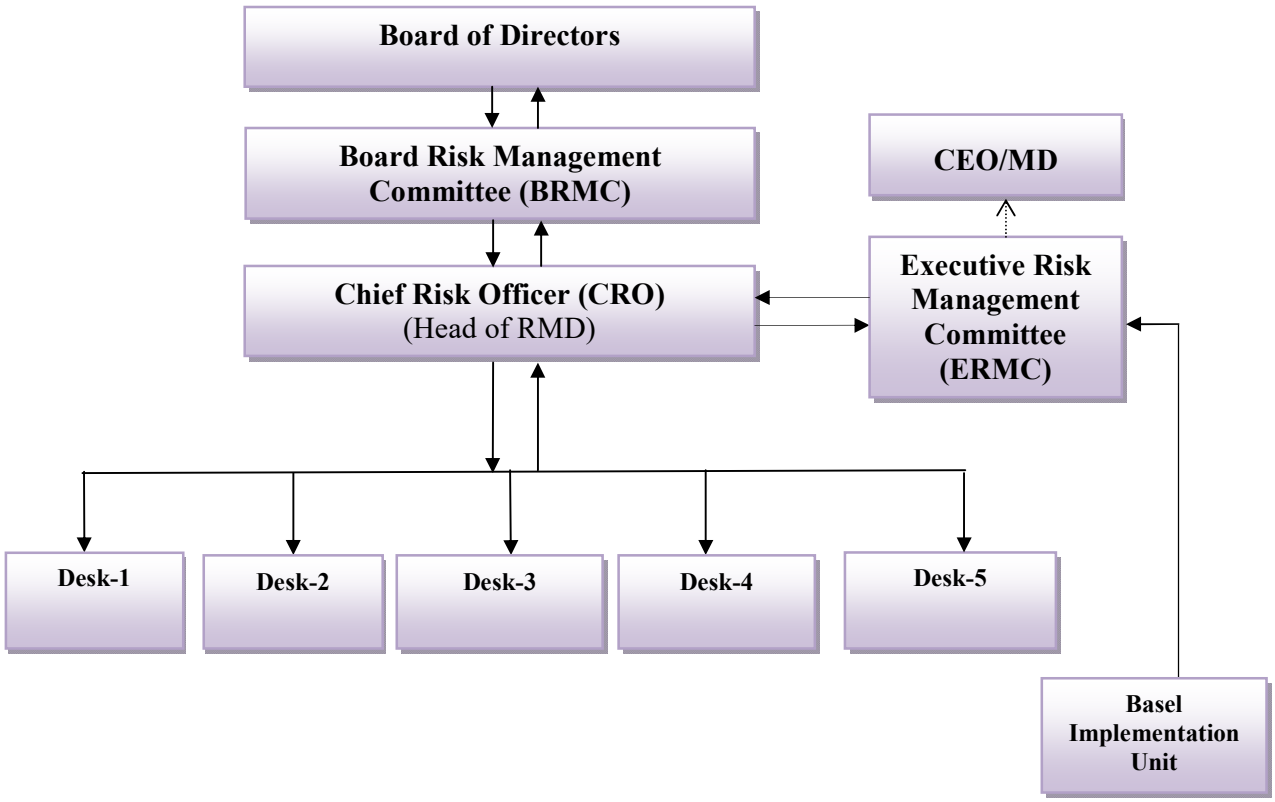
a) Establishing and maintaining an effective system of internal controls, including the enforcement of official lines of authority and the appropriate segregation of duties.
b) Having a properly structured system of internal controls for promoting effective operations, providing reliable financial reporting, safeguarding assets and ensuring compliance with relevant laws, regulations and internal policies.
c) Evaluating the adequacy of the internal control environment considering the following factors:

    i) the appropriateness of the system in relation to the type and level of risks;
    ii) clear lines of authority and segregation of duties across the organization;
    iii) sufficient independence of the control functions;
    iv) the reliability, accuracy and timeliness of all financial, operational and regulatory reports;
    v) the adequacy of procedures for ensuring compliance with applicable laws, regulations and internal policies and procedures;
    vi) review of internal controls and information systems;
    vii) adequate documentation of coverage, procedures, findings and management responses to audits;
    viii) appropriate and timely attention to identified material weaknesses and objective verification and review of management's actions to correct those deficiencies.

2.7 Optimal Risk Management Organogram

Below is the organogram that should be followed by all scheduled banks operating in the country. Each bank is given the flexibility to enhance the organogram according to their size and complexity. When the banks will formulate their own risk management policy guidelines,

they should name the various desks specifically in the organogram. If the bank wants, they can give functional designation to the officials according to the risk areas they are assigned to:



2.7.1 Role of Board of Directors

The board of directors of the bank shall give utmost importance on sound risk management practices. They will take every possible initiative to keep various risks (credit, market, liquidity, operational risks etc.) within tolerable level. For this purpose the board will play the following roles:

a) Establishing organizational structure for enterprise risk management within the bank and ensuring that top management as well as staffs responsible for risk management possess sound expertise and knowledge to accomplish the risk management function properly;
b) Assigning sufficient authority and responsibility to risk management related officials;
c) Ensuring uninterrupted information flow to RMD for sound risk management;

d) Continuously monitoring the bank's performance and overall risk profile through reviewing various reports;
e) Ensuring the formulation, review (at least annually) and implementation of appropriate policies, plans and procedures for risk management;
f) Defining and reviewing the risk appetite, risk tolerance, limit etc. in line with strategic planning;
g) Making sure maintenance of adequate capital and provision to absorb losses resulting from risk;
h) Ensuring that internal audit reviews the credit operations, foreign exchange operations and securities portfolio management functions etc. to assess the effectiveness of internal control system;
i) Monitoring the function of Board Risk Management Committee.

2.7.2 Role of Board Risk Management Committee (BRMC) in addition to but not excluding the role defined in the related BRPD circular

a) Formulating and reviewing (at least annually) risk management policies and strategies for sound risk management;
b) Monitoring implementation of risk management policies & process to ensure effective prevention and control measures;
c) Ensuring construction of adequate organizational structure for managing risks within the bank;
d) Supervising the activities of Executive Risk Management Committee (ERMC);
e) Ensuring compliance of BB instructions regarding implementation of core risk management;
f) Ensuring formulation and review of risk appetite, limits and recommending these to board of directors for their review and approval;
g) Approving adequate record keeping & reporting system and ensuring its proper use;
h) Holding at least 4 meetings in a year (preferably one meeting in every quarter) and more if deemed necessary;
i) Analyzing all existing and probable risk issues in the meeting, taking appropriate decisions for risk mitigation, incorporating the same in the meeting minutes and ensuring follow up of the decisions for proper implementation;
j) Submitting proposal, suggestions & summary of BRMC meetings to board of directors at least on quarterly basis;
k) Complying with instructions issued from time to time by the regulatory body;
l) Ensuring appropriate knowledge, experience, and expertise of lower-level managers and staffs involved in risk management;
m) Ensuring sufficient & efficient staff resources for RMD;
n) Establishing standards of ethics and integrity for staffs and enforcing these standards;

o) Assessing overall effectiveness of risk management functions on yearly basis. Banks are encouraged to preserve video recording of the BRMC meetings for verification by the team from Bangladesh Bank (DOS) involved in monitoring risk management activities. The team may meet the members of BRMC and ERMC of the bank from time to time to get a closer perspective of risk management culture and practice.

2.7.3 Role of Executive Risk Management Committee (ERMC)

Bank shall form ERMC comprising of CRO (as the Chairman), Head of ICC, CRM/CAD, Treasury, AML, ICT, ID, Operation, Business, Finance, Recovery and Head of any other department related to risk if deemed necessary. RMD will act as secretariat of the committee. The ERMC, from time to time, may invite top management (CEO, AMD, DMD, Country heads or senior most executives), to attend the meetings so that they are well aware of risk management process. The responsibilities/Terms of Reference of ERMC will include, but limited to:

a) Identifying, measuring and managing bank's existing and potential risks through detailed risk analysis;
b) Holding meeting at least once in a month based on the findings of risk reports and taking appropriate decisions to minimize/control risks;
c) Ensuring incorporation of all the decisions in the meeting minutes with proper dissemination of responsibilities to concerned divisions/departments;
d) Minimizing/controlling risks through ensuring proper implementation of the decisions;
e) Reviewing risks involved in new products and activities and ensuring that the risks can be measured, monitored, and controlled adequately;
f) Submitting proposals, suggestions & summary of ERMC meetings to CEO, BRMC on regular basis;
g) Implementing the decisions of BRMC and board meetings regarding risk issues;
h) Assessing requirement of adequate capital in line with the risk exposures and ensuring maintenance of the same through persuading senior management and board;
i) Determining risk appetite, limits in line with strategic planning through threadbare discussions among the members;
j) Contributing to formulation of risk policies for business units;
k) Handling "critical risks" (risks that require follow-up and further reporting);
l) Following up reviews and reports from BB and informing BRMC the issues affecting the bank's operation;
m) Ensuring arrangement of Annual Risk Conference in the bank.

2.7.4 Chief Risk Officer (CRO)

In banking institution, the Chief Risk Officer (CRO) is responsible for ensuring intense and effective risk management across the organization. The CRO works to ensure that the bank is

compliant with rules, regulations, and reviews factors that could negatively affect the bank's objectives. According to the Basel Committee on Banking Supervision, CRO has been referred as an independent senior executive with distinct responsibility for the risk management function and the institution's comprehensive risk management framework across the entire organization.

2.7.4.1 Appointment of CRO

Bank shall appoint Chief Risk Officer (CRO) who will act as the head of Risk Management Department. Appointment, dismissal and other changes to the CRO position should be approved by the board or its risk management committee. If the CRO is removed from his/her position, this should be disclosed publicly. The bank should also discuss the reasons for such removal with its supervisor. CRO's performance and compensation should be reviewed and approved by the board or its risk management committee.

Bank shall consider the following criteria as a minimum for appointing CRO:

1) Senior executive having mainstream banking experience preferably covering
    i. Core risk management
    ii. Internal Control and Compliance
    iii. Capital management
    iv. Branch banking
    v. Core banking system
    vi. Risk based certification

2) Minimum three years hands on working experience in risk management
3) The position of the CRO should be one grade higher than or at-least equal to the heads of other departments for effective risk management.

2.7.4.2 Role of CRO

To bring better transparency, synergy and prudence into risk management structure in the bank, the role and responsibilities of the CRO is of paramount significance. The CRO leading the independent risk management department shall have sufficient stature, authority and seniority. He or she shall have direct access to the board of directors and make direct reports to the board or its Risk Management Committee. He or she is to be directly supervised by the Board Risk Management Committee (BRMC). CRO should not have any reporting relationships with business verticals of the bank and should not be given any business targets. CRO shall provide all the key risk issues prevailing in the bank to BRMC meetings and a copy to the CEO for acknowledgement. The CRO must have access to any information necessary for performing his/her duties. In this context board and CEO/MD will provide full support to him/her.

CRO of a bank shall undertake the following responsibilities, but not limited to, in order to ensure transparency in managing risks at all levels:

- To oversee the development and implementation of the bank's risk management functions as a primary role;
- To support the Board of Directors/Board's Risk Management Committee in its development of the bank's risk appetite and for translating the risk appetite into a risk limits structure;
- To actively engage with the management in the process of setting risk appetite and limits for the various business lines with a view to achieve bank's overall strategic planning and monitoring their performance relative to risk-taking and limit adherence;
- To contribute and participate in key decision-making processes (i.e. strategic planning, capital and liquidity planning, new products and services, compensation design and operation);
- To manage the implementation of all aspects of the risk function, including implementation of processes, tools and systems to identify, measure, manage, monitor and report risks;
- To assist in the development of and manage processes to identify and evaluate business risks and control them;
- To manage the process for developing risk management policies and procedures, risk limits and approval authorities;
- To monitor major and critical risk issues independently with full empowerment;
- To communicate views of the board and senior management throughout the bank;
- To adopt proper financial protection measures through risk transfer, risk avoidance, and risk retention programs;
- To provide opinion regarding extent of risk in case of credit proposal for big amounts (to be set by the bank) before submission to EC/board for sanctioning;
- To monitor portfolio health and ensure good quality asset growth;
- To ensure proper compliance of BB's recommendations regarding risk issues including all core risks;
- To provide a methodology to identify and analyze the financial impact of loss to the organization, employees, the public, and the environment;
- To disseminate information and strategies to personnel regarding emerging risk issues and industry specific risks;
- To implement environmental and social (E&S) safeguard for the asset portfolio;
- To oversee the information security aspects for the bank;
- To ensure arrangement of ERMC meeting on monthly basis wherein top management team shall address, discuss and resolve risk issues across the bank;
- To ensure proper disclosure of key performance indicators of the bank via Pillar III of Basel III accords;

- To remain aligned and acquainted with other countries' economic and financial positions;
- To organize Annual Risk Conference (at-least one day-long) with the participation of all the branch managers and deputy branch managers including the officials related to risk issues;
- Ensuring adequate internal and external training on risk management issues for increasing efficiency of RMD officials.

It is to be mentioned that CRO should not be given dual responsibility, more specifically the responsibility of Chief Operating Officer, Chief Financial Officer, Chief of the internal audit function or any other function.

2.7.5 Risk Management Division/Department (RMD)

Banks must have an independent full-fledged risk management department/division. The Risk Management Division/Department (RMD) shall be headed by the Chief Risk Officer (CRO). It should have separate desks within the risk management department for overseeing each key risk area. The main functions of the department include, but not limited to, the followings:

- managing the process for developing risk policies and procedures;
- coordinating with business users/units to prepare functional specifications;
- preparing and forwarding risk reports; and
- assisting in the implementation of all aspects of the risk function.

The risk management function shall be functionally and hierarchically independent from business and other operation functions. The officials who take and own risks should not be given responsibility for monitoring and evaluating their risks. Safeguards against conflict of interest should be put in place to maintain independence of the risk management function. Sufficient resources should be provided to Risk Management Department where the personnel possess 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 carry out its crucial function effectively.

According to the business size and nature of activity, the bank will form various desks under the Risk Management Department to perform its assigned activities. However, necessary desks under the division should be as follows:

1) Credit Risk
2) Market Risk
3) Liquidity Risk
4) Operational Risk
5) Risk Research and Policy Development

It is noted that there is a negative relationship between capital and bank risk, i.e. when the capital increases, the bank risk decreases. Hence, there must be a close relationship and communication between Basel Implementation Unit (BIU) and RMD.

2.7.5.1 Scope of Work of RMD

- Involvement of RMD officials limited to risk management related activities
- Involvement of RMD in annual budget/strategy meeting
- Internal risk assessment (annually)
- Access to any information related to risk throughout the bank
- Request to ICC Division to conduct audit on any specific issue if deemed necessary
- Membership of all important committees like SMT, ALCO, CCD, Credit Risk Committee, Budget committee, Basel Implementation Committee etc. But RMD's role will be only as an observer and to raise flags on risk issues but not be part of decision making process.

2.7.5.2 Role of RMD

The RMD needs to manage and measure risks on the basis of the bank's approved risk parameters independently in line with regulatory requirements. The role of RMD includes, but not limited to, the followings:

- Collecting and analyzing data/information for identifying risks and making appropriate recommendations for risk mitigation;
- Preparing risk management reports, arranging monthly meeting of ERMC and preparing meeting minutes, disseminating the decisions to the concerned department/divisions, monitoring and follow up of implementation status;
- Ensuring timely submission of risk management reports, meeting minutes, compliance report and other documents to BB;
- Assisting BRMC/ERMC by providing risk issues that are needed to be addressed;
- Designing bank's overall risk management strategy;
- Ensuring significant contribution in establishing sophisticated risk management infrastructure with a sufficiently robust data-base, data architecture and information technology;
- Conducting, developing and overseeing Stress Testing activity;
- Utilizing the Stress Test result and scenario analysis to better understand potential risk exposures under a variety of adverse circumstances;
- Developing and testing different models (such as VaR, HHI index, Collection scoring, Vintage curve etc.), and observe their use for measuring and monitoring risks;

- Assisting senior management in formulating strategic planning considering bank's risk exposures and industry as a whole;
- Supporting the board, BRMC and ERMC in formulation, review and approval of the enterprise-wide risk governance framework which includes the bank's risk culture, risk appetite, risk limits, and MAT;
- Monitoring on ongoing basis the risk-taking activities and risk exposures in line with the board approved risk appetite, risk limit and corresponding capital or liquidity needs (i.e. capital planning);
- Taking initiatives for interim review of risk appetites on request of other related departments and informing the board of directors and BRMC time to time about the status of risk exposures as compared to appetite;
- Establishing an early warning or trigger system for breaches of the bank's risk appetite or limits;
- Communicating views of the board and senior management throughout the bank;
- Taking initiatives for establishing enterprise/comprehensive risk management policies and procedures with the approval of the board;
- Monitoring concerned departments in formulating and reviewing related risk management policies and procedures;
- Monitoring compliance of irregularities found in core risk inspection reports of BB;
- Adopting proper financial protection measures through risk transfer, risk avoidance, and risk retention programs;
- Taking appropriate steps to control or mitigate risk exposures and ensure reporting the same to senior management and BRMC.

RMD of the bank is encouraged to prepare a comparative analysis report on bank's gain/loss due to/lack of proper risk management activities and its impact on capital and send the same to senior management & board of the bank and DOS of BB on yearly basis.

2.7.5.3 Desk-wise Functions of RMD

For smooth functioning of risk management activities, the desks of RMD should commonly do the following tasks:

All the desks are individually responsible for collecting the related data/information, progress report of the previously taken decisions of ERMC and BRMC from concerned divisions/department for proper risk analysis and identification of risks, making appropriate recommendations, preparing memo on related issues, monitoring and following up of implementation status of the decisions of meeting minutes, ensuring regulatory compliance on related issues, assisting in formulation and review of risk appetite and risk related policies/guidelines. The desks are also responsible for monitoring the associated risks through concerned department/divisions.

In addition, the desks will perform the following specific tasks:

Credit Risk related desk

- Assisting in formulation and review of credit risk management policies, guidelines, manual, setting up of credit risk appetite, limit, tolerance, MAT etc. with due consideration for sector, industry, geographical location, regulatory limits, best practices, current business and economic conditions;
- Monitoring loan portfolio to ensure good quality asset growth;
- Monitoring credit concentration and ensuring compliance of internal limit;
- Closely monitoring the stressed loans to avoid adverse classification;
- Monitoring and following up overdue loans, SMA loans, NPL, law suit cases, written off loans, regular accounts with unsatisfactory repayment, loans having excess over limit, overdue accepted bills, off-balance sheet exposures, forced loans, movement of adverse classification, collateral against loans, credit rating of borrowers, taken over loans etc.;
- Using different models for identifying related risks;
- Maintaining liaison with independent internal loan review desk as per revised CRM guidelines and ensuring its proper functioning.
- Conducting Stress Testing activity to understand shock resilience capacity of the bank;
- Analyzing Stress Testing report, finding out the vulnerable areas that are needed to be addressed and accordingly advising the same to senior management and board to ensure maintenance of adequate capital for absorbing any unforeseen losses.

Market Risk related desk

- Ensuring that the treasury department calculates interest sensitive assets and liabilities properly for determining the impact of interest rate fluctuation on the profitability of the bank;
- Measuring interest rate risk of the bank by applying various tools such as sensitivity analysis, duration gap analysis etc.;
- Monitoring foreign exchange related risk such as exchange rate risk, maintenance of FX related limits, repatriation of export proceeds, outstanding of overdue accepted bill, reconciliation of long pending Nostro account transaction etc. through concerned departments;
- Measuring equity price risk by using various tools like VaR and monitoring the same to keep market exposure safe and sound;
- Conducting Stress Testing activity to understand shock resilience capacity of the bank;

- Analyzing Stress Testing report, finding out the vulnerable areas that are needed to be addressed and accordingly advising the same to senior management and board to ensure maintenance of adequate capital for absorbing any unforeseen losses.

Liquidity Risk related desk

Treasury is primarily responsible for managing liquidity risk. Since RMD is responsible for overseeing enterprise level risk, it will ensure proper implementation of the instructions laid down in the ALM guidelines such as maintenance of regulatory requirements of liquidity ratios, liquidity forecasting etc. For doing this, the desk will perform the following activities:

- Ensuring that the treasury department prepares Structural Liquidity Profile, projected sources and uses of fund, statement of total time and demand liabilities and calculates all regulatory liquidity ratios such as CRR, SLR, ADR, LCR, NSFR, MCO, WBG, Undrawn Commitment etc.;
- Regularly monitoring liquidity ratios, liability concentration, growth of asset and liability including off-balance sheet items, asset-liability of off-shore banking unit etc. to manage liquidity risk;
- Playing major role in setting liquidity strategy;
- Assessing opportunity loss resulted from improper liquidity management;
- Conducting Stress Testing activity to understand shock resilience capacity of the bank;
- Analyzing Stress Testing report, finding out the vulnerable areas that are needed to be addressed and accordingly advising the same to senior management and board to ensure maintenance of adequate capital for absorbing any unforeseen losses.

Operational Risk related desk

- Identifying the vulnerable areas related to operational risk in collaboration with ICC and suggesting the senior management and board to review the existing policies to prevent recurrences of the unexpected incidents;
- Assisting in managing risks related to lapses in people, process and system;
- Monitoring unsettled issues (identified fraud/forgeries, major irregularities etc.) through ICC;
- Playing an important role to uphold the reputation of the bank by minimizing operational risks.

Risk Research and Policy Development desk

- Developing, testing, and using different models (such as VaR, Collection scoring, Vintage curve etc.) for measuring/assessing risks;

- Reviewing effectiveness of enterprise-wide risk governance framework and recommending necessary policy measures;
- Conducting research to explore reasons behind concurrence of the identified risks and suggesting the senior management probable ways to control the same;
- Exploring emerging risks and recommending preventive measures to achieve the organizational goal;
- Assisting senior management in formulating strategic planning considering bank's risk exposures and industry as a whole;
- Preparing a consolidated Risk Appetite Statement (RAS) based on the information provided by the related divisions/departments;
- Developing the KRI reporting format based on the complexity and size of the bank, suggesting mitigating measures to concerned departments based on the KRI provided by them, preparing summary of KRI and submitting the same to BRMC on quarterly basis.

2.8 The Concept of Risk Appetite

The risk management framework is expected to be developed and applied within an overarching statement of risk appetite. Risk appetite along with risk tolerance and risk threshold are to be set and approved by the board. The risk appetite must reflect strategic planning of the bank which includes shareholder aspirations within the constraints of regulatory requirements, creditor and legal obligations.

A strategic plan is a document reflecting the mission and strategic goals of a bank, generally for a period of at least five years. A good strategic plan must be clear, consistent with goals, flexible, and adjustable to changes in the environment. A bank must have a board approved strategic plan for ensuring the substantial growth and lead the bank in an efficient and logical way.

A strategic plan should contain, at least the followings, but not limited to:

a) Analysis of the external environment in which the bank operates, including the SLEPT (Socio-cultural, Legal, Economic, Political and Technological analysis) analysis;
b) Critical review of the institutional performance including SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis;
c) Bank's strategic goals and objectives;
d) Corporate Governance;
e) Compliance with laws and regulations;
f) Strengthening Internal Control & Compliance and Review System;
g) Optimization of operating expenses;

h) Reducing Non-performing loans;
i) Increasing NPL recovery;
j) Deposit growth with a view to optimizing cost of fund;
k) Lending growth with industry and business segment focus;
l) Maintaining adequate capital for absorbing all material losses;
m) Maintaining optimum liquidity;
n) Risk Appetite Statement for all material risks;
o) Human resources development;
p) Automation and effective Management Information System (MIS);
q) Proactive risk management and governance.

2.8.1 Definition of Risk Appetite

Risk appetite is the level and type of risk a bank is able and willing to assume in its exposures and business activities, given its business objectives and obligations to stakeholders (depositors, creditors, shareholders, borrowers, regulators). Risk appetite is generally expressed through both quantitative and qualitative means and should consider extreme conditions, events, and outcomes. It should be stated in terms of the potential impact on profitability, capital and liquidity.

2.8.2 Risk Appetite Objectives

In support of the bank's mission, the risk appetite focuses mainly on the following five overarching risk management objectives:

- Upholding the highest ethical standards of conduct;
- Preserving the long-term financial resilience of the bank;
- Avoiding losses when investing public money;
- Ensuring compliance with legal and regulatory obligations;
- Maintaining a robust internal control environment and safeguarding operational continuity.

2.8.3 Risk Appetite Framework

The science of developing and adopting a risk appetite framework (RAF) is still evolving at banks all over the world. Some banks have adopted a high-level, brief, and qualitative statement of RAF, while others have made it complex, lengthy, and quantitative. Risk appetite is the cornerstone of a successful risk management framework.

Risk appetite framework should include the following criteria:

- Be reviewed and approved by the board of directors at least annually;
- Be in line with the organization's strategy, objectives and key stakeholders' demands;
- Cover all key risks discussing risk preferences both in terms of risks that are sought out and risks that should be minimized;
- Clearly document risks as part of a risk register, including risk-specific definitions, risk owner, how and how often each risk will be measured, assumptions related to each risk, judgment on severity and likelihood, and speed at which risks could manifest;
- Recognize that losses occur and are part of business but include loss tolerances that are reflective of overall business objectives;
- Reflect the human and technological resources needed to measure and manage the bank's risks in a timely fashion.

2.8.4 Developing Risk Appetite Statement

Developing a risk appetite statement is a complex endeavor and is both art and science. The steps in its development include:

- Start with the bank's overall strategic and financial objectives.
- Consider annual reports and financial statements, regulatory requirements, Peer group and industry-wise growth, bank's own portfolio growth, trend of NPL, profitability and capital, liquidity position, risk management culture and practices etc.
- Determine the bank's risk profile.
- Set tolerances for exposures and potential losses in consultation with the business line and related departments.
- Get board approval and communicate it throughout the organization.

- In preparing Risk Appetite Statement (RAS), banks are required to set the loan growth target in line with its strategic objectives and mention it in both absolute amount and percentage form. For example, if a bank wants to make 20% loan growth in a particular year to achieve its strategic planning/objective, it should state the percentage of loan growth along with increased amount of loans. In this regard, banks have to mention at least previous three years' real performance along with the current year risk appetite, tolerance and limit. The expected loan growth/amount is also to be distributed in each sector, industry and regional area under the head of Risk Appetite, Risk Tolerance and Risk Limit/Threshold. Risk appetite should be measurable and subject to time consideration for periodic review and must have risk treatments. In case of interim review (if necessary), the revised appetite statement shall have to be approved by the board of directors and submitted to DOS of BB and communicated throughout the organization. However, repeated review of risk appetite statement is discouraged.

2.8.5 Areas of Risk Appetite

Banks shall prepare risk appetite statement covering all regulatory requirements related to risks, components of pillar II under Basel III, strategic planning and all other probable risks exist in the bank. For example, in setting appetite for liquidity risks they should look into the ratios laid down in the ALM guidelines and related circulars issued by BB. In addition, the banks shall also consider the CRMR report in setting the above limits. Apart from the regulatory requirements, the banks should set risk appetite, tolerance and limit for all the probable areas of risks. Possible areas for setting risk appetite are as follows:

- Overall growth of total loans and advances including off-balance sheet item
- Credit concentration (borrower/sector/geographical area wise)
- Gross and net NPL to total loans
- Cash recovery against classified loans/written off loans
- Amount of loan outstanding with acceptable rated customers (ECA score up to 3) to the amount lies with total rated customers
- Unsecured exposure* to total exposure (funded)
- Rescheduled loans to total classified loans
- Written off loans to total classified loans
- Interest waiver as % of NPL
- Impact on Net Interest Income (NII) due to adverse change in interest rate
- Bucket-wise gap under simple sensitivity analysis for interest rate change
- Exchange rate shock to operating income
- Value at Risk (VAR) for securities and FX
- Overdue accepted bills (payable and receivable) to total loans
- Net Open Position limit
- Exchange rate shock to operating income
- Liability concentration (Top-10 deposit suppliers to total deposit)
- Bucket-wise gap under structural Liquidity Profile (SLP)
- Liquidity ratios (at least for regulatory requirements) including Commitment Limit and Wholesale Borrowing Guideline (WBG) Limit
- Loss due to overall operational risk
- Loss due to internal and external fraud
- Operational loss due to employment practice and workplace safety, clients, products, and business practice, damage to physical assets, business disruption and system failure, execution, delivery and process management

* Unsecured exposure is the exposure against which no eligible collateral (defined by BB) is held.

- Expected operational loss as % of operating income
- Operating expenses to operating income
- CRAR including CRAR after combined minor shock
- Credit rating of bank itself
- CAMELS rating
- Core risks rating
- Regulatory ratios

Banks shall set risk limit for regulatory issues in line with the thresholds laid down by BB but they are encouraged to apply their own prudence for determining/fixing the maximum/minimum perimeter for those issues considering their risk taking capacity, risk management practices etc. For example, bank having trouble with liquidity should follow more stringent/conservative measure and set the limit for AD ratio below the regulatory threshold.

Chapter 3

Risk Management Process

3.1 Risk Management Process

Banks shall comply with the latest core risk guidelines and risk management guideline circulated by BB for effective risk management. They will develop and implement their own guidelines and various types of risk management tools in consistent with the complexity, size and nature of business, risk strategy and BB guidelines. The risk strategy should be determined taking into consideration bank's capital adequacy, expected level of profitability, market reputation, adequacy and experienced personnel, logistic support, macro and micro economic scenario, risk management practices etc. The board of directors, senior management and other officials of the bank should be aware of and understand their respective responsibilities within the risk management system.

An effective risk management system includes the implementation of clearly defined policies and processes to facilitate the identification and quantification of risks inherent in a bank's different activities. The policy should be formally established and approved by the board of directors and should clearly set out the parameters under which different risks are to be managed/controlled.

3.2 Steps of Risk Management Process

Risk management is an iterative process that, with each cycle, can contribute progressively to organizational improvement by providing management with a greater insight into risks and their impact. It is a series of multi-steps that, when undertaken in sequence, enable continual improvement in decision-making.

Steps of Risk Management Process in a Banking Organization:

Step 1 – Communicate and Consult
Step 2 – Establish the context
Step 3 – Identify the risks
Step 4 – Analyze the risks
Step 5 – Evaluate the risks
Step 6 – Treat the risks
Step 7 – Monitor the risks

Step-1: Communication and Consult

This is preparatory step that aims to identify the responsible persons involved in risk assessment (including identification, analysis and evaluation) and also the persons engaged in the treatment, monitoring and review of risk.

In this step, management must communicate the roles, responsibilities, accountabilities of the internal stake holders. Formation of policies, review/revision, and dissemination of the policies is also part of this step. Risk owners/originator should be informed of his/her/their role when dealing with the risks. All the stake holders should be communicated after due consultation that everybody should inform and notify RMD as and when they identify something to be noted in the risk register as potential risk to be addressed. This information to RMD officials should preferably be in black and white or even through e-mail. RMD officials will then include the item in the risk register.

Step-2: Establishment of the context

This is another preparatory stage that closes to starting the formal risk management process. Before risk can be clearly understood and dealt with, it is important to understand the context in which it exists.

The steps to assist establishing the context within which risk will be identified are:

a) Establish the internal context

Under this sub-step, the objectives and goals of a business or activity must first be identified to ensure that all significant risks are understood. This ensures that risk decisions always support the broader goals and objectives of the business. This approach encourages long-term and strategic thinking.

b) Establish the external context

This sub-step defines the overall environment in which the bank operates. An analysis of these factors will identify the strengths, weaknesses, opportunities and threats to the business in the external environment. Local and global issues are also important to be considered.

c) Establish the risk management context

It is important to define the limits, objectives, appetite and scope of the activity or issue under examination. For example, in conducting a risk analysis for a new product or project loan, such as the introduction of a new branch, wing of banking business or a new product line, it is important to clearly identify the parameters for this activity to ensure that all significant risks are identified.

Step-3: Risk Identification

The next step is to identify possible risks that may affect, either negatively or positively, the objectives of the business and the activity under analysis. The purpose of this step is to identify what could go wrong (likelihood) and what is the consequence (loss or damage) of its occurring.

There are two main ways to identify banking risks:

1. **Identifying retrospective risks**

Retrospective risks are those that have previously occurred, such as incidents or accidents.

Methods of identifying retrospective risks include:

- Audit reports
- Various risk reports
- Regular reports
- Hazard or incident logs or registers
- Customer complaints
- Changes in regulations
- Past employee survey/exit interview
- Media reports (print or electronic)
- Bangladesh Bank inspection report

2. **Identifying prospective risks**

Prospective risks are those that have not yet happened, but might happen sometime in future.

Methods for identifying prospective risks include:

- Brainstorming with staff or external stakeholders
- Researching the economic scenario (macro or micro both local and global)
- Conducting interviews with the relevant people and/or organizations
- Undertaking surveys of staff or clients to identify anticipated issues or problems or risks
- Reviewing policy, process, systems

Step -4: Analysis of the risks

The risk analysis step assists in determining which risks have a greater consequence or impact than others. Thus, analyzing the likelihood and consequences of each identified risk and deciding which risk factors will potentially have the greatest effect, it should, therefore, receive priority with regard to how they will be managed. The level of risk is analyzed by combining estimates of likelihood (table 1) and consequences (table 2).

It is important to consider the consequences and the likelihood of risk in the context of the size, complexity, objective of the activity of a banking company is pursuing. It is important to note that the likelihood/frequency and also the impact/consequence will vary from bank to bank.

Table 1– Likelihood scale

Rating	LIKELIHOOD The potential for problems to occur in a year
5	ALMOST CERTAIN: will probably occur, could occur several times per year
4	LIKELY: high probability, likely to arise once per year
3	POSSIBLE: reasonable likelihood that it may arise over a five-year period
2	UNLIKELY: plausible, could occur over a five to ten year period
1	RARE: very unlikely but not impossible, unlikely over a ten year period

Table 2 – Loss or damage impact scale

Rating	POTENTIAL IMPACT **In terms of the objectives of the Bank**
5	CATASTROPHIC: most objectives may not be achieved, or several severely affected
4	MAJOR: most objectives threatened, or one severely affected
3	MODERATE: some objectives affected, considerable effort to rectify requires medical attention and has some impact on overall health of the bank and also may impact on the economy the bank is operating in
2	MINOR: easily remedied, with some effort the objectives can be achieved
1	NEGLIGIBLE: very small impact, rectified by normal processes

Step -5: Evaluation of the risks

Risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria, and deciding whether these risks require treatment. The result of a risk evaluation is a prioritized list of risks that require further action. This step is about deciding whether risks are acceptable or need treatment.

Step-6: Treatment of risks

Risk treatment is about considering options for treating risks, evaluating those options, preparing the risk treatment plans and implementing those plans to achieve the desired outcome.

- Options for treatment need to be proportionate to the significance of the risk, and the cost of treatment commensurate with the potential benefits of treatment. Risk treatment should also aim to enhance positive outcomes.

- **Options for risk treatment**

  It identifies the following options that may assist in the minimization of negative risk or an increase in the impact of positive risk.

  1. Avoid the risk
  2. Change the likelihood of the occurrence
  3. Change the consequences
  4. Share the risk
  5. Retain/Accept the risk supported by the CRAR as per Basel III

  In fact, the options are the followings and can be applied either individually or in combination:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.
- Accepting and retaining the risk by making informed decision and having plans for managing and funding the consequences of the risk if it occurs.
- Reducing the likelihood of the risk through staff training, changing procedures, or by reducing the impact through diversifying credit portfolio, setting up off-site data backup etc.
- Sharing the risk with another party or parties through insurance, consortium financing, etc.

Step-7: Monitoring and review of risks

Risks need to be monitored periodically to ensure changing circumstances do not alter the risk priorities. Very few risks will remain static, therefore, the risk management process needs to be regularly repeated, so that new risks are captured in the process and effectively managed.

A risk management plan at every business level should be reviewed at least on an annual basis. An effective way to ensure that is to combine risk planning or risk review with annual business planning.

Risk management should be fully incorporated into the operational and management processes at every level of the organization and should be driven from the top down.

3.3 KRI/Risk Register:

The KRI is one of the effective tools for comprehensive risk management that should be maintained by each bank to identify the key business and financial risks, to define and implement respective controls/mitigating factors to reduce the risks faced by the bank and its subsidiaries. Business Line managers shall report the key risks issues to RMD as and when identified/detected. RMD should review the KRI based on the reports provided by the line managers, RMD will suggest mitigation measures to concerned units and also submit the effectiveness of the mitigation measures to BRMC on quarterly basis.

Minimum components of risk register should be as follows:

1. Date: As the risk register is a living document, it is important to record risk identification date, target date and completion dates for treating risks
2. Risk Number: A unique identifying number of the risk
3. Risk Description: A brief description of the risk, its causes and impact
4. Existing Controls: A brief description of the controls that are currently in place for the risk
5. Consequence: The consequence (severity or impact) of rating for the risk, using scales (e.g. 1-5 with 5 being most severe)
6. Likelihood: The likelihood (probability) rating for the risk, using scales (e.g. 1-5, with 5 being most likely)
7. Overall risk score: Determined by multiplying likelihood (probability) times consequence (Impact) for a scale ranging from 1-25
8. Risk Ranking: A priority list which is determined by the relative ranking of the risk by their overall risk score
9. Trigger: Something which indicates that a risk is about to occur or has already occurred
10. Management Action: Action which is to be taken if the risk found adverse
11. Risk Owners: The person(s) for whom the risk is being generated or is supposed to look after the situation before the risk is generated (mainly business line personnel).

Management of credit, market, liquidity and other risks

In managing credit, market, liquidity and operational risks, banks shall follow the latest core risk management guidelines on Credit, Foreign Exchange, Asset-Liability (including appendix), Internal Control & Compliance, ICT Security and Prevention of Money Laundering and Terrorist Financing.

Banks are encouraged to develop different tools and models for measuring credit, market and liquidity risks. For example: GINI Coefficient, Herfindahl–Hirschman Index (HHI) for measuring concentration risk, Credit Risk Modeling for measuring expected loss, Interest Rate Sensitivity and Duration Analysis for interest rate risk, VaR for equity and FX risk, Stress Testing for credit, market and liquidity risk, Structural Liquidity Profile for liquidity risk etc.

Chapter 4

Operational Risk Management

4.1 Introduction

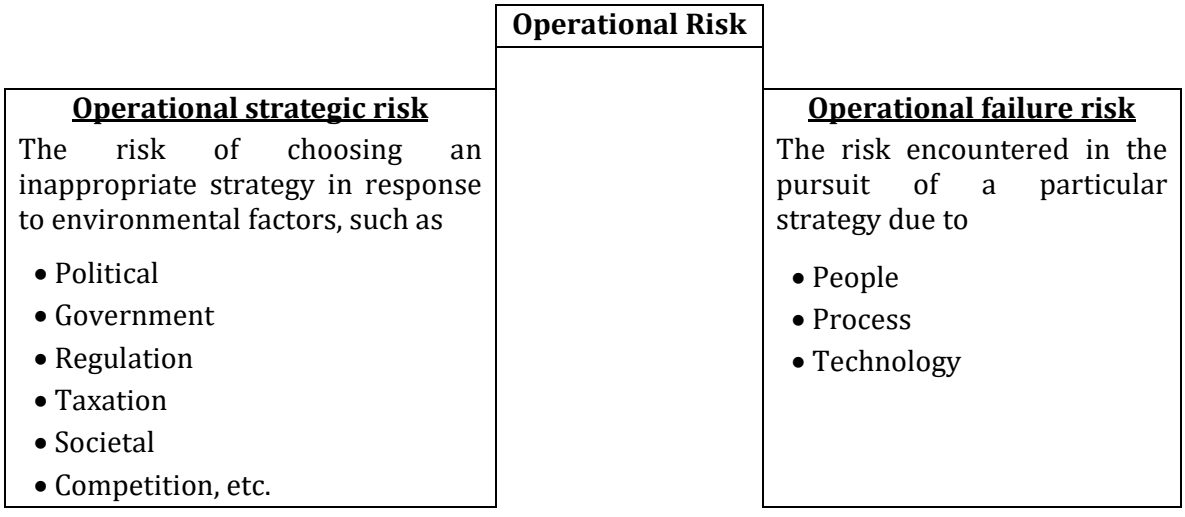
Operational risk is defined as the risk of unexpected losses due to physical catastrophe, technical failure and human error in the operation of a bank, including fraud, failure of management, internal process errors and unforeseeable external events.

It is clear that operational risk differs from other risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and that this affects the risk management process. At the same time, failure to properly manage operational risk can result in a misstatement of a bank's risk profile and expose the bank to significant losses.

Operational risk can be subdivided into two components: operational strategic risk and operational failure risk. It is also defined as internal operational risk.

Operational strategic risk arises from environmental factors such as a new competitor that changes the business paradigm, a major political and regulatory regime change, and other factors that are generally outside the control of the bank. It also arises from a major new strategic initiative, such as getting into a new line of business or redoing how current business is to be done in the future. It is also defined as external operational risk.

Operational failure risk arises from the potential for failure in the course of operating the business. A firm uses *people*, *process*, *and technology* to achieve business plans, and any one of these factors may experience a failure of some kind. Accordingly, operational failure risk is the risk that exists *within* the business unit caused by the failure of people, process, systems or technology. A certain level of the failures may be anticipated and should be built into the business plan. These failures can be expected to occur periodically, although both their impact and their frequency may be uncertain.



4.2 Categorization of Operational Risk

Banks are required to adopt and utilize standard categorizations of operational risk events, according to Event Type and Business Line. Not all Business Lines will be relevant for all banks. There are seven major Event Types, and eight major (Level 1) Business Lines, and within each combination of Event Type and Business Line, there may be one or more Scenario Descriptions. The following list of Scenario Descriptions, categorized by Event Type and Business Line, represent the largest scenarios most frequently reported by banks. For any bank, it is unlikely, but possible, that some of the scenarios may occur under business lines in addition to the ones reported in the table.

Event Type	Business Line	Scenario Descriptions
Type A: Internal Fraud	Corporate Finance	Loan Fraud Embezzlement Failure to follow procedures/limits
	Trading & Sales	Unauthorized trading/rogue trader Misappropriation of assets Breach of trading limits
	Retail Banking	Theft of customer data/information Embezzlement Theft of assets
	Commercial Banking	Fraudulent transfer of funds Embezzlement Theft of customer funds
	Payment and Settlement	Payment fraud Theft of client funds or assets
	Asset Management	Unauthorized trading activities
	Not allocated to any business line	Embezzlement Misuse of confidential information Misappropriation of assets
Type B: External Fraud	Corporate Finance	Client misrepresentation of information Theft Loan fraud
	Trading & Sales	Loan fraud Cybercrime Forgery
	Retail Banking	Cybercrime Check fraud Theft of information/data

Event Type	Business Line	Scenario Descriptions
	Commercial Banking	Fraudulent transfer of funds Credit product fraud (loans, L/C, guarantees)
	Payment and Settlement	Payment fraud
	Not allocated to any business line	Loan fraud Cybercrime Robbery
Type C: Employment Practices and Workplace Safety	Trading & Sales	Discrimination Occupational accident
	Retail Banking	Occupational accident Discrimination Environmental issue
	Not allocated to any business line	Pandemic Wrongful termination Discrimination
Type D: Clients, Products, and Business Practices	Corporate Finance	Regulatory breach Compromised customer information Fiduciary breach
	Trading & Sales	Fiduciary breach Regulatory breach Compromised customer information
	Retail Banking	Regulatory breach Mis-selling Compromised customer information
	Commercial Banking	Noncompliance with money laundering regulations Regulatory breach Mis-selling
	Asset Management	Mis-selling
	Not allocated to any business line	Client suitability Noncompliance with money laundering regulations
Type E: Damage to Physical Assets	Trading & Sales	Business continuity failure Damage to building and premises
	Retail Banking	Fire Flood Damage to building and premises

Event Type	Business Line	Scenario Descriptions
	Commercial Banking	Damage to building and premises Natural disaster
	Not allocated to any business line	Natural disaster Terrorist attack Vandalism Earthquake
Type F: Business Disruption and System Failure	Trading & Sales	IT system failure
	Retail Banking	IT system failure Utility outage
	Commercial Banking	Off-shoring/Outsourcing risk IT system failure
	Payment and Settlement	IT system failure Failure of payments infrastructure
	Agency Services	IT system failure
	Asset Management	IT system failure
	Not allocated to any business line	IT system failure
Type G: Execution, Delivery, and Process Management	Corporate Finance	Inaccurate/Incomplete contract Transaction error Staff error in lending process
	Trading & Sales	Data entry error Model risk
	Retail Banking	Pricing error Failure of external supplier
	Commercial Banking	Failure to follow procedures Lost or incomplete loan/legal documentation Processing error Collateral management error
	Payment and Settlement	Data entry error Failure to follow procedures
	Agency Services	Processing error
	Asset Management	Mismanagement of account assets
	Not allocated to any business line	Unapproved access given to client accounts Inaccurate financial statement Failure of supplier/vendor Tax noncompliance

4.3 Operational Risk Management Framework

An operational risk management framework should be based on an appropriate definition of operational risk, which clearly articulates what constitutes operational risk in the bank. The framework should cover the bank's tolerance for operational risk, as specified through the policies for managing this risk and the bank's prioritization of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the bank. It should also include policies outlining the bank's approach to identifying, assessing, monitoring and controlling/mitigating the risk. The degree of formality and sophistication of the bank's operational risk management framework should be commensurate with the bank's risk profile. There should be separation of responsibilities and reporting lines between operational risk control functions, business lines and support functions in order to avoid conflict of interest. The framework should also articulate the key processes the bank needs to have in place to manage operational risk.

4.4 Board Oversight

The board is responsible for creating an organizational culture that places high priority on effective operational risk management and adherence to sound operating controls. Operational risk management is most effective where a bank's culture emphasizes high standards of ethical behavior at all levels of the bank. The board should promote an organizational culture, which establishes through both actions and words the expectations of integrity for all employees in conducting the business of the bank. Generally, the board should at least:

a) Establish tolerance level and set strategic direction in relation to operational risk. Such a strategy should be based on the requirements and obligation to the stakeholders of the bank;
b) Approve the implementation of a bank-wide framework to explicitly manage operational risk as a distinct risk to the bank's safety and soundness;
c) Provide senior management clear guidance and direction regarding the principles underlying the framework and approve the corresponding policies developed by senior management;
d) Establish a management structure capable of implementing the bank's operational risk management framework specifying clear lines of management responsibility, accountability and reporting; and
e) Review the operational risk management framework regularly to ensure that the bank is managing the operational risks. This review process should also aim to assess industry best practice in operational risk management appropriate for the bank's activities, systems and processes.

4.5 Senior Management Oversight

The senior management should at least:

a) Translate the operational risk management framework established by the board into specific policies, processes and procedures that can be implemented and verified within different business units;
b) Clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability and ensure that the necessary resources are available to manage operational risk effectively;
c) Assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy;
d) Ensure that bank activities are conducted by qualified staffs with necessary experience, technical capabilities and access to resources, and that staffs responsible for monitoring and enforcing compliance with the bank's risk policy have authority and are independent from the units they oversee;
e) Ensure that the bank's operational risk management policy has been clearly communicated to staffs at all levels of the organization that are exposed to material operational risks.

4.6 Policies, Procedures and Limits

Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes and procedures related to advanced technologies supporting high transaction volumes, in particular, should be well documented and disseminated to all relevant personnel.

The bank should put in place an operational risk management policy. The policy should include at least, but not limited to, the followings:

a) The strategy given by the board of the bank;
b) The systems and procedures to set up effective operational risk management framework; and
c) The structure of operational risk management function and the roles and responsibilities of individuals involved.

The policy should establish a process to ensure that any new or changed activity, such as new products or systems conversions, will be evaluated for operational risk prior to coming into effect. It should be approved by the board and documented. Senior management should ensure that it is clearly communicated and understood to staffs at all levels in units that are

exposed to material operational risks. Senior management also needs to place proper monitoring and control processes in order to have effective implementation of the policy. The policy should be regularly reviewed and updated, to ensure it continues to reflect the environment within which the bank operates.

Banks should also establish policies for managing the risks associated with outsourcing activities. Outsourcing activities can reduce the bank's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialized business activities. However, a bank's use of third parties does not diminish the responsibility of the board and senior management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing institution. Furthermore, banks need to manage residual risks associated with outsourcing arrangements, including disruption of services. Firms that utilize third-party vendors to provide services with which customers come into direct contact (such as a partnership with a mobile network operator to allow customers to transfer funds via SMS) need to exercise caution so that service interruptions do not damage the reputation of the bank.

4.7 Risk Assessment and Quantification

Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems and its vulnerability to these risks. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures**.** While a number of techniques are evolving, operating risk remains the most difficult risk category to quantify. It would not be feasible at the moment to expect banks to develop such measures. However, the banks could systematically track and record frequency, severity and other information on individual loss events. Such data could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control that risk.

Effective risk assessment allows the bank to better understand its risk profile and most effectively target risk management resources. Amongst the possible tools that may be used by banks for identifying and assessing operational risk are:

(a) **Self risk assessment:** A bank assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and should be based on approved checklists to identify the strengths and weaknesses of the operational risk environment.

(b) **Risk mapping**: In this process, various business units, organizational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritize subsequent management actions.

(c) **Risk indicators**: Risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators are to be reviewed on a periodic basis (such as monthly or quarterly) to alert banks to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions. Threshold/limits could be tied to these indicators such that when exceeded, could alert management on areas of potential problems.

(d) **Historical data analyses:** The use of data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events. Banks may also combine internal loss data with external loss data (from other banks), scenario analyses, and risk assessment factors.

4.8 Mitigation of Risks

Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled, e.g. natural disasters. Risk mitigation tools or programs can be used to reduce the exposure to, or frequency and/or severity of such events. For example, insurance policies can be used to externalize the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

However, banks should view risk mitigation tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly recognize and rectify legitimate operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk e.g. legal or counterparty risk.

Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses.

The later may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the bank's immediate control, e.g. external events. Such problems may cause serious difficulties for banks and could jeopardize a bank's ability to conduct key business activities. Banks should, therefore, establish disaster recovery and business continuity plans that address this risk.

4.9 Risk Monitoring

An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities help quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event. There should be regular reporting of pertinent information to senior management and the board that supports the proactive management of operational risk. Senior management should establish a program to:

a) Monitor assessment of all types of operational risk faced by the bank;
b) Assess the quality and appropriateness of mitigating actions, review effectiveness of the same periodically; and
c) Ensure that adequate controls and systems are in place to identify and address problems before they become major concerns.

It is essential that:

i. Responsibility for the monitoring and controlling of operational risk should follow the same type of organizational structure that has been adopted for other risks, including market and credit risk;
ii. Senior management ensure that an agreed definition of operational risk together with a mechanism for monitoring, assessing and reporting is designed and implemented; and
iii. This mechanism should be appropriate to the scale of risk and activity undertaken.

In addition to monitoring operational loss events, banks should specify and identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators or operational risk matrix) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system failure, and so on. When thresholds are directly linked to these indicators, an effective monitoring process can help identifying key material risks in a transparent manner and enable the bank to act upon these risks appropriately. Regular reviews should be carried out by internal audit, or other qualified parties, to analyze the control environment and test the effectiveness of implemented controls, thereby ensuring business operations are conducted in a controlled manner.

The results of monitoring activities should be included in regular management and board reports as compliance reviews performed by the internal audit and risk management functions.

4.10 Risk Reporting

Senior management should ensure that information is received by the appropriate people, on a timely basis, in a form and format that will assist in the monitoring and control of the business. The reporting process should include information such as:

a) The critical operational risks facing, or potentially facing, by the bank;
b) Risk events and issues together with intended remedial actions;
c) The effectiveness of actions taken;
d) Details of plans formulated to address risk issues;
e) Areas of stress where crystallization of operational risks is imminent; and
f) The status of steps taken to address operational risk.

The operational risk reports should contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be distributed to appropriate levels of management and to areas of the bank on which concerns may have an impact. Reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of these reports, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports.

Reports should be analyzed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

In general, the board should receive sufficient higher level information to enable them to understand the bank's overall operational risk profile and focus on the material and strategic implications for the business.

4.11 Establishing Control Mechanism

Control activities are designed to address the operational risks that a bank has identified. For all material operational risks that have been identified, the bank should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely. To be effective, control activities should be an integral part of the regular activities of a bank. A framework of formal, written policies and procedures is necessary; it needs to be reinforced through a strong control culture that promotes sound risk management practices.

4.12 Contingency Planning

Banks should have disaster recovery and business continuity plans to ensure its ability to operate as a going concern and minimize losses in the event of severe business disruption. The business disruption and contingency plans should take into account different types of scenarios to which the bank may be vulnerable and should be commensurate with the size and complexity of its operations. Management should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. Plan should be tested periodically to ensure that they are likely to be effective in case of need.

4.13 Internal Controls

Internal control systems should be established to ensure adequacy of the risk management framework and compliance with a documented set of internal policies concerning the risk management system. Principal elements of this could include, for example:

a) Top-level reviews of the bank's progress towards the stated objectives;
b) Checking for compliance with management controls;
c) Policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
d) A system of documented approvals and authorizations to ensure accountability to the appropriate level of management.

Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. Board and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a bank.

Operational risk can be more pronounced where banks engage in new activities or develop new products (particularly where these activities or products are not consistent with the bank's core business strategies), enter unfamiliar markets, and/or engage in businesses that are geographically distant from the head office. It is, therefore, important for banks to ensure that special attention is given to internal control activities including review of policies and procedures to incorporate such conditions.

Banks should have in place adequate internal audit coverage to ensure that policies and procedures have been implemented effectively. The board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit program is appropriate to the risk exposures. Audit should periodically validate that the bank's operational risk management framework is being implemented effectively across the bank.

To the extent that the audit function is involved in oversight of the operational risk management framework, the board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the operational risk management process. The audit function may provide valuable input to those responsible for operational risk management, but should not have direct operational risk management responsibilities.

An effective internal control system also requires existence of appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to individuals, or a team, may enable them to conceal losses, errors or inappropriate actions. Therefore, areas of potential conflict of interest should be identified, minimized, and subjected to careful independent monitoring and review.

In addition to segregation of duties, banks should ensure that other internal practices are in place as appropriate to control operational risk.

Chapter 5

Capital Management

5.1 Capital Management and Its Relationship with Risk Management

Capital management in a bank usually refers to implementing measures aimed at maintaining adequate capital, assessing internal capital adequacy of the bank and calculating its capital adequacy ratio. It is gaining increasing importance around the world, as reflected from taking several reform initiatives and changes in the prudential requirements undertaken by banks in different countries in line with the reform measures proposed by the Basel Committee on Banking Supervision.

Risk management is increasingly becoming difficult to separate from capital management. Most banking risks can be quantified as numerical indicators, and this quantification naturally leads to the principle that increased capital can be held to cover unexpected losses at a certain confidence level. The followings indicate the relationship between risk management and capital requirement:

a) Capital management helps to ensure that the bank has sufficient capital to cover the risks associated with its activities;
b) As part of the internal capital adequacy assessment process (ICAAP), management identifies the risks that the bank is exposed to, and determines the means by which they will be mitigated;
c) Capital is used to cover some of these risks, and the remainder of these risks is mitigated by means of collateral or other credit enhancements, contingency planning, additional reserves and valuation allowances, and other mechanisms.

The outcomes of capital management are:

i. A Capital Plan that meets the needs of the bank over a longer time horizon;
ii. An ICAAP that determines precise levels of required capital (the "solvency need") according to the measures of balance sheet capital and regulatory capital;
iii. A process to regularly compare available capital with current and projected solvency needs, and address deficiencies in a timely manner.

5.2 Framework of Capital Management

Banks will devise and establish suitable capital management systems in order to calculate the capital adequacy ratio and secure adequate capital to cover the risks they face, from the standpoint of ensuring soundness and appropriateness of the their businesses. In this regard, banks shall follow the latest guidelines on Risk Based Capital Adequacy and related BB circulars/instructions to assess its capital adequacy.

Roles and responsibilities at various levels as well as the framework of capital management are outlined as below:

5.2.1 Roles and Responsibilities of Board of Directors and Senior Management

The Board of Directors and Senior Management will take the following steps:

(1) Define the goals of capital management in an official policy statement. Such goals must include the followings:
   a) Regulatory compliance, such that capital levels always exceed BB's requirements;
   b) Capital levels that are aligned with the risks in the business and consistent with the strategic plan; and
   c) Appropriate capital level that maintains balance between maximizing shareholder returns and protecting the interests of depositors and other creditors.

(2) Integrate capital management into the bank's strategic plan taking into account the fact that lack of the same could jeopardize the achievement of the bank's strategic objectives. Annually, conduct a detailed strategic planning process over a three-year time horizon, the outcomes of which are embodied in a Strategic Plan. The planning process should include forecasting key economic variables which business lines may use in allocating resources. New strategic initiatives to be undertaken over the planning period and their financial impact are then determined;

(3) These planning processes are used then to review capital ratios, targets, and levels of different classes of capital against the bank's risk profile and risk appetite. The board must be satisfied that capital levels under specific stressed economic scenarios are sufficient to remain above both BB and the bank's internal requirements;

(4) Review the policies and specific measures for developing and establishing an adequate capital management system with a full grasping of the assessment, monitoring and control techniques of internal capital adequacy as well as the significance of capital management;

(5) Disseminate the capital management policies throughout the bank. The policies should be inclusive of the following matters:

   a) The roles and responsibilities of the Board of Directors, executive risk management committee and Basel Implementation Unit (BIU) of the bank with regard to capital management;
   b) Basic policies for maintaining sufficient capital and on the capital allocation process;
   c) Policy on the risk limits in relation to the capital;
   d) The definition of capital and risk as used in the Internal Capital Adequacy Assessment Process (ICAAP);

e) Calculation of the capital adequacy ratio in line with capital adequacy guidelines issued by Bangladesh Bank; and
f) Methods of internal capital adequacy assessment in conducting capital allocation process, and the basis for the calculation of capital to be allocated to risks.

(6) Analyze present as well as future capital needs of the bank and adopt suitable capital-raising methods, satisfying the prudential and regulatory requirements of BB;

(7) Ensure consistency of the capital management system with the bank's risk profile and the competing business environment;

(8) Set an appropriate level of capital target for the short-term, medium-term and long-term and develop a Capital Plan to achieve the target. The Capital Plan must identify the capital issuance requirements and options around capital products, such as the issuance of common equity, timing and markets to execute the Capital Plan under different market and economic conditions. The following factors should be taken into account in setting the capital targets:

a) BB's regulatory capital requirements;
b) Coverage of unexpected losses up to a certain probability of occurrence (economic capital);
c) Expected asset growth and profitability;
d) Dividend policy;
e) Stress test scenarios;
f) The basis for the calculation of capital to be allocated to risk;
g) Capital management rules exhaustively covering the arrangements necessary for the ICAAP and the calculation of the capital adequacy ratio and the arrangements befitting the scale and nature of the bank business and its risk profile;

h) Consistency of the definition of capital used in the ICAAP and the bank's corporate management policy and plans, its strategic objectives, etc.;

i) The basis for determining the definition of capital as used in the ICAAP in reference to capital as defined under regulations concerning capital adequacy ratios-Tier 1, Tier 2 capital, and eligible capital; (To update the literature in terms of Basel III)

j) Keeping the BIU, with close relationship with RMD, in charge of the ICAAP and the calculation of the capital adequacy ratio independent from other offices/divisions and secure a check-and-balance system;

Chapter 6

Risk Management Reporting

6.1 Risk Management Reporting

After proper analysis, risks are to be prioritized and reported to competent authorities (both internal and external) by RMD on regular basis.

Banks shall prepare Monthly Risk Management Report (MRMR) and Comprehensive Risk Management Report (CRMR) according to the formats provided by BB as a minimum requirement. They can also include additional information related to the concerned risk areas depending on the nature, complexity and size of business. Banks shall arrange monthly meeting of ERMC to discuss the risk issues based on the findings of the risk reports prepared by the RMD and shall submit the CRMR and MRMR along with the minutes of ERMC meeting to DOS of BB within stipulated time. Discussions & decisions of ERMC must be reflected in the meeting minutes. Banks shall also submit the board approved Risk Appetite Statement (RAS) on yearly basis and BRMC meeting minutes on regular basis. Besides they shall submit a soft copy of Stress Test report to DOS of BB on half yearly basis along with risk reports. The risk reports and forwarding letter are to be signed by the CRO.

In addition to the above reporting requirements, all banks must submit review report (board resolution copy) of Risk Management Policies and effectiveness of risk management functions with the approval of the board of directors to DOS of BB on yearly basis.

6.2 Penalty for Non-Compliance

If a bank's employee willfully/knowingly furnishes false information in reporting to BB, such an offence is punishable under section 109(2) of the Bank Company Ain 1991. BB may impose penalty as per section 109(7) of the said Ain if a bank fails to submit the above mentioned reports within stipulated time without any acceptable/satisfactory reason.

Glossary

Risks are the potential that an uncertainties, event, action or inaction will adversely impact the ability of an entity to achieve its organizational objectives. In this definition, uncertainties include events which may or may not happen as well as uncertainties caused by ambiguity or a lack of information.

Risk management framework is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. The notion of a risk management framework is essentially equivalent to the concept of Enterprise Risk Management (ERM).

Risk culture is about understanding risks the financial institution faces and how they are managed. A sound and consistent risk culture throughout a financial institution is a key element of effective risk management. Risk culture and its impact on effective risk management must be a major concern for the board and senior management.

Risk appetite is the amount and type of risk an organization is prepared to pursue or take, in order to attain the objectives of the organization and those of its shareholders and stakeholders.

Risk capacity is the amount and type of risk an organization is able to support in pursuit of its business objectives.

Risk tolerance(s) is/are quantified risk criteria or measures of risk exposure that serve to clarify and communicate risk appetite. Risk tolerances are used in risk evaluation in order to determine the treatment needed for acceptable risk.

Risk target is the optimal level of risk that an organization wants to take in pursuit of a specific business goal.

Risk limit is a measure of risk, either expressed in terms of (gross) exposure or possible loss or in another metric that tends to correlate with exposure or possible loss. Being a limit, this measure of risk is articulated as an indication of risk tolerance with the intention to constrain risky activities or positions within an entity to an acceptable level.

Risk exposure designates a gross measure of risk, before taking account of risk mitigation and before applying any particular knowledge about the probability of loss events that would activate the exposure.

Risk severity is determined by the size of the possible loss or the gravity of the impact, in the event that a certain risk should materialize. It does not imply any particular knowledge about how likely or frequent such an event might be.

Risk profile is the amount or type of risk a financial institution is exposed to. Forward Risk Profile is a forward looking view of how the risk profile may change both under expected and stressed economics conditions.

Risk governance refers to the structure, rules, processes, and mechanisms by which decisions about risks are taken and implemented. Risk governance covers the questions about what risk management responsibilities lie at what levels and the ways the board influences risk-related decisions; and the role, structure, and staffing of risk organization.

Bibliography

1. Corporate governance principle for banks, BCBS, July,2015.
2. https://www.ausport.gov.au/__data/assets/word_doc/0005/454928/Risk_Management_process.doc