Risk Management Guidelines

2019

AGRANI BANK LIMITED
www.agranibank.org

Agrani Bank Limited
Risk Management Division
Head Office, Dilkusha C/A, Dhaka-1000

Risk Management Guidelines-2019

Working Committee

Advisors

Md. Anisur Rahman, Deputy Managing Director

Md. Rafiqul Islam, Deputy Managing Director

Chairman

Md. Monowar Hossain, General Manager (Head of ICC), Agrani Bank Limited, Head Office, Dhaka

Member Secretary

Mahmudul Ameen Masud, General Manager (Risk Management), Agrani Bank Limited, Head Office, Dhaka

Members & panel of editors

1. Sukanti Bikash Sanyal, General Manager (PRL), Agrani Bank Limited
2. Md. Enamul Mowla, Deputy General Manager, IT&MIS Division (IT), Agrani Bank Limited, Head Office, Dhaka
3. Md. Shahidul Islam, Deputy General Manager, Islamic Banking Unit, Agrani Bank Limited, Head Office, Dhaka
4. Biswajit Das, Assistant General Manager, Risk Management Division, Agrani Bank Limited, Head Office, Dhaka
5. K B M Rajibul Hasan, Senior Principal Officer, Risk Management Division, Agrani Bank Limited, Head Office, Dhaka

Preamble

To strengthen risk management activity of the bank, Bangladesh Bank (BB) issued risk management guidelines for banks in 2012 which has been revised in 2018 with a view to upgrade the initiatives to manage various risks and to ensure sound risk management culture in the bank. As per BB directives, each Bank shall prepare its own guidelines approved by the Board and shall submit a copy to the Department of Off-site Supervision (DOS) for information. This guideline is subjected to review at least once a year for adapting with the changing environment.

The guideline outlines actions for ensuring proper identification, measurement, timely treatment of risks and implementation of the issues incorporated. Bank must also ensure compliance the following reports to DOS (Department of Offsite Supervision) of BB within the stipulated time frame as mentioned below:-

- Soft copies of risk management reports (CRMR in June & December and MRMR on monthly basis for all other months) for successive months of each quarter as well as minutes of monthly Executive Risk Management Committee (ERMC) meeting within the next month of the reporting quarter;
- Board Risk Management Committee(BRMC) meeting minutes within 7 days of the meeting held;
- Board approved Risk Appetite Statement (RAS) on yearly basis within first two months of the year;
- A soft copy of Stress Test report on half yearly basis along with CRMR;
- 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.

Table of Contents

Table of Contents

Table of Contents

List of Graphs and Tables

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

BOD Board of Directors

BIU Basel Implementation Unit

BRMC Board Risk Management Committee

CRAR Capital to Risk Weighted Asset Ratio

CRM Credit Risk Management

CRMR Comprehensive Risk Management Reporting

CRO Chief Risk Officer

ERMC Executive Risk Management Committee

ICC Internal Control & Compliance

MCO Maximum Cumulative Outflow

MIS Management Information System

NPL Non Performing Loans

OBS Off-Balance Sheet

RAS Risk Appetite Statement

RMD Risk Management Division

RWA Risk Weighted Asset

SLP Structural Liquidity Profile

SWOT Strengths, Weaknesses, Opportunities, Threats analysis

VaR Value at Risk

WBG Wholesale Borrowing Guidelines

OBJECTIVE OF RISK MANAGEMENT

1.1 Introduction

This risk management guideline has been prepared in accordance with the Guidelines on Risk Management for Banks issued by Department of Off-site Supervision of Bangladesh Bank (BB) for all scheduled Banks of Bangladesh vide DOS Circular No. 04, dated 08-10-2018. As such the guideline is also Applicable for Agrani Bank Limited (ABL) in all of its Branches and Subsidiaries, Zonal offices, Circle offices, Islamic Banking Windows and all Head office divisions.

The purpose of this guideline is to set out the principles for all the Branches, Subsidiary units, Zonal offices, Circle offices and Divisions of ABL of its key risks. The risks covered are credit risk, market risk, liquidity risk, operational risk, strategic risk and compliance risk. The principles of this Risk Management Guideline are subject to regular update and amendment, as required and amendments to be approved by the Board of Directors.

The guideline is structured to set the Bank's risk-taking into the context of its mission and strategy as well as to its risk-bearing capacity and willingness to take various risks. The Bank's risk governance structure is described with focus on key risk responsibilities. The Guidelines for risk management are implemented through principles, limits, operational guidelines as well as methodologies and tools for risk measuring, monitoring and reporting. Together these form the Bank's risk management framework.

1.2 Objectives

The objectives of ABL in publishing the Risk Management Guideline are:

1. To promote a sound risk culture at all levels of the bank
2. To establish the standard for the risk management practices
3. To improve the financial soundness of bank
4. To develop a sound risk management framework
5. To introduce risk management tools and techniques for assessment and necessary treatment of various risks

1.3 Risk Management Dimension

Risk management is the process that identifies loss exposures faced by an organization and selects the most appropriate techniques for treating such exposures. The dimensions of risk management involve development of risk culture, risk strategy and risk appetite, risk governance, risk assessment and treatment.

1.3.1 Risk Culture

Risk culture is the norms and traditions of behavior of all level of employees within the Bank that determine the way in which they identify, understand, manage the risks considering risk tolerance and appetite. A sound risk culture encourages effective risk management, promotes sound risk-taking and ensures that risk-taking activities beyond the Bank'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.

To develop a sound and consistent risk culture, employees at all levels of ABL must follow the latest risk management guidelines of the bank and be trained regarding their responsibilities for risk. Business and operational units of ABL have the primary responsibility for managing risk on day-to-day basis, considering risk tolerance and risk appetite, and in line with Bank's risk guidelines and procedures.

1.3.1.1 The risk culture of ABL can be strengthened through the following:

- Enabling an open and respectful atmosphere in which employee feel encouraged to speak up when observing new or excessive risks;
- Clarify the range of acceptable risks using an embedded risk appetite statement and various forms of communication and training;
- Aligning incentives with objectives and clarifying how breaches in policies/procedures will be addressed.

1.3.2 Risk Strategy and Risk Appetite

Since the total business of Bank involves risk taking, ABL has set the risk appetite and risk limit in major indicators as per instruction of BB. Risk appetite is the level of risk that the Bank is prepared to accept while risk tolerance relates to the actual limits that the Bank has set. Risk appetite statement plays an important role in passing the risk strategy down through the institution.

ABL has strategy to achieve long term and short-term goals and objectives. Along with business goals, bank needs to 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.

A good practice of risk management process 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.

1.3.3 Risk Governance and Organization

The risk governance structure outlines the key responsibilities for decisions on risk taking and risk oversight in the Bank. The board of directors is the Bank's supreme decision-making body. It oversees bank's affairs and provides sound leadership for the CEO and management. Authorized by the Board, various Board committees oversee specific responsibilities based on clearly defined terms of reference. Under the risk management approach of the bank, the Board, through the Board Risk Management Committee (BRMC), sets risk appetite which is approved by board of Directors, oversees the establishment of enterprise-wide risk management policies and processes, and sets risk appetite limits to guide ABL's risk-taking. The BRMC oversees the identification, monitoring, management and reporting of credit, market, liquidity, operational and reputational risks. Besides, Executive Risk Management Committee (ERMC) has the responsibility to execute the risk management policies and processes prescribed by BRMC.

The Chief Risk Officer (CRO), who is the head of ERMC (Executive Risk Management Committee) and a member of BRMC, oversees the risk management functions, recommends and monitors the Bank's risk appetite and policies, and follows up risk related issues. The CRO is responsible for the following:

- Management of bank's risks, including systems and processes to identify, approve, measure, monitor, control and report risks
- Engagement with senior management about material matters regarding all risk types
- Development of risk controls and mitigation processes
- Ensuring bank's risk management process is effective, and the Risk Appetite established by the Board is adhered to.

Risk governance of ABL follows a three-lines-of-defense model.

The first line of defense- business and operation units (Branches, Zones), own and manage risks. They have responsibilities to identify, assess measure, monitor, mitigate, and report on their risks according to the risk policies and delegation power. The units are also responsible for having skills, operating procedures, systems, and controls in place to ensure their compliance with risk policies and delegation power.

The second line of defense is put in place to support senior management by bringing expertise and monitoring alongside the first line to ensure that risks and controls are properly managed. The following activities are included in this level of defense:

- Supporting management policies, defining roles and responsibilities, and setting goals for implementation.
- Providing risk management frameworks.
- Identifying shifts in the organization’s implicit risk appetite.
- Assisting management in developing processes and controls to manage risks and issues.
- 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 audit is considered as the third line of defense of bank 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.

1.3.4 Risk Assessment and Treatment

The ultimate responsibility for risk assessment lies solely with the bank. Risk management process is the systematic application of management policies, procedures and practices to the assessment, treatment, controlling, and monitoring of risk. The process is the integral part of management, embedded in the culture and practices, and tailored to the business process of the organization. The risk management process should include proper risk assessment and treatment as described below:

1.3.4.1 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 crucial activities. Risk identification includes identification of nature of risk, sources of risk, cost of risk, areas of impacts, events, their causes and their potential consequences. The risk may arise from both existing and new business which must be recognized and understood at initial stage. Otherwise, those risks will not be included in further analysis.

Risk analysis involves developing an understanding of the risk. It provides an input to risk evaluation and decisions on the most appropriate strategies and techniques for risk treatment. The risk analysis of ABL involves measuring risk by considering consequences of an unfavorable event and likelihood of such event occurring. While analyzing, bank considers the factors that affect consequences and likelihood of the nature of risk, severity of risk; and the information, data and resources available. Risk analyses are two types in nature, such as quantitative and qualitative. ABL has used some tools to quantify most of the risks. However, bank adopts qualitative measures to capture reputational and operational risks as these are difficult to quantify.

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.

1.3.4.2 Risk Treatment

After the assessment of exposed risk, bank chooses the best option to eliminate or mitigate unacceptable risks according to the policies and guidelines. There are several methods of handling the risks:

- Avoiding the risk by deciding not to start or continue with the activity that gives risk to the risk.

- Loss control consists of certain activities that reduce both the frequency and severity of losses. Loss control has two major objectives: loss prevention and loss reduction. Loss prevention aims at reducing the probability of loss so that the frequency of losses is reduced. Bank reduces 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.

- Retention means that the Bank retains all or part of a given 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.

- Noninsurance transfers are another technique of bank for handling risk. The risk is transferred to another bank by several methods, such as hedging, swap, contract, options.

- Insurance is the pooling of fortuitous losses by transfer of such risks to insurers, who agree to indemnify insured for such losses, to provide other pecuniary benefits on their occurrence, or to render services connected with the risk. Bank transfers some of its risks through insurance.

Selection of 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 bank to address risks is to put in place adequate risk control mechanisms. Bank establishes and communicates risk limits through policies, standards and procedures that define responsibilities and authority. These limits help to know when the risk becomes unacceptable and align their actions and behaviors with the risk appetite, risk tolerance, and strategy.

To ensure effective measures of risk treatment plan, ABL continues monitoring and review which encompass all aspects of risk management process for the purposes of followings:

- 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.

Bank develops and applies its risk management framework within an encompassing risk appetite statement in the volatile and risk-driven financial condition. Setting a risk appetite is embracing risks in areas where management has the skills, knowledge and experience whilst limiting or eliminating of risks in other areas. The risk appetite replicates the strategic planning which includes stakeholders' aspiration within the constraints of regulatory requirements, legal obligations etc.

RISK MANAGEMENT SYSTEM

Risk management system includes policies, procedures, limits, and controls to provide adequate, timely, and continuous identification, assessment, measurement, monitoring, mitigation, and reporting of risks posed by its activities at the operational layers.

The success of risk management in bank depends on the effectiveness of the risk management system. The system should be comprehensive enough to capture all the material risks to which the institution is exposed and 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 encompass the following:

- ❑ Active involvement of board and senior management;
- ❑ Adequate organization, policies and procedures;
- ❑ Appropriate management information systems; and
- ❑ Comprehensive internal controls and limits.

Risk management functions are not only limited to the Risk Management Division/Department (RMD). Business lines (the branches, zones, Units, Subsidiaries and circles) 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, the following features should, at least, be present in the bank:-

- ❑ Submission of various reports to the Board and senior management incorporating different types of risks, risk mitigation measures, comparison of risk levels with limits, the level of capital required for absorbing losses, and suggestions for restoring capital;
- ❑ Consistency between the risks taken by the management and risks perceived by Board;

- Active, bank-wide risk management approach that includes all operational layers;
- Alignment of treasury functions with risk management;
- Efficient and effective management of asset and liability;
- Active management of contingent liabilities;
- Using both firm-specific and market-wide stress scenarios for liquidity management;
- Taking the stress testing result into consideration to understand the impact of adverse scenario on the bank's profitability or capital;
- Independent risk management function with sufficient authority, logistic support and continuous communication with business lines;
- Experienced and expert personnel for performing risk management activities;
- Giving importance to 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. The overall responsibility for risk management is rest with the board of directors. The senior management should be aware of the activities undertaken by the bank that could expose it to various risks, considers the bank's risk profile on an ongoing basis and 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.

Thus, Board needs to approve the strategies and significant risk management policies developed by management of the bank and review them on regular basis. Board of directors need not be involved in day-to-day activities of risk management rather they oversee the risk management functions of the bank.

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 needs to be aware of the activities undertaken in the bank and possess necessary knowledge and skills to align the risk levels with the board's strategies through risk assessment and treatment. Top management also needs to be aware of the bank's risk profile on an ongoing basis and regularly report it to the board or a board level committee for review.

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.

2.4 Policies, procedures and limit structure

The board of directors and senior management formulates and implements risk management policies and procedures to deal with various risks that arise from the bank's business and operational activities. Bank's internal policies and procedures formulated for operating different functions work as guidance for the day-to-day implementation of broad risk strategies, and include limits designed to shield the bank from imprudent and unwarranted risks. These policies and procedures include not only specific risk areas like Credit Policy, Liquidity Management Policy, and Operational Risk Management Policy, but also overall risk management activities. The management reviews risk policies, procedures, and limits in a timely manner as prescribed in regulatory guidelines and update them when necessary.

To ensure adequacy of policies, procedures and limits, the following key factors needs to be considered:-

a) Proper documentation of policies, procedures and limits considering the risks associated with the activity, review and approval by the appropriate internal authority (line management and board);

b) Assignment of full accountability and delegation of authority in the policies for each functional area (Operational layers that are directly involved with the associated risk areas) ; and

c) Development of compliance monitoring procedures incorporating internal compliance checks for adherence to all policies, procedures and limits by internal control unit (bank has a separate Internal Control & Compliance division in place to monitor and supervise the internal control system).

2.5 Risk measurement, monitoring and management reporting systems

Agrani Bank Limited performs the following key activities to ensure effective risk measurement, monitoring and management reporting systems:-

a) Identifying and measuring all quantifiable and material risk factors (as mentioned in regulatory framework and in internal policies) through proper information systems to provide 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 management 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 data sources, procedures, analysis and documentation; adequacy of information technology or management information system environment; consistency in management information reporting and other forms of communication; compliance with set limits,; 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 bank. Comprehensive internal control structure helps management understand risks and ensure that conditions within the level commensurate with the risk appetite, risk tolerance, risk limit and strategy. A major part of the internal control structure is 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.

ABL's internal control system is performed and reviewed by Internal Control & Compliance Division (ICCD). The coverage, procedures, and findings of the audit regarding the internal controls are reviewed by the Audit Committee of the board and any material weakness found is addressed promptly and appropriately.

Activities to be performed to ensure internal control environment in the bank:-

a) Effective system of internal controls, including the enforcement of official lines of authority and the appropriate segregation of duties.

b) 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) Adequacy of the internal control environment considering the following factors:

i) The appropriateness of the control system in relation to the type and level of risks;

ii) Reliability, accuracy and timeliness of all financial, operational and regulatory reports;

iii) The adequacy of procedures for ensuring compliance with applicable laws, regulations and internal policies and procedures;

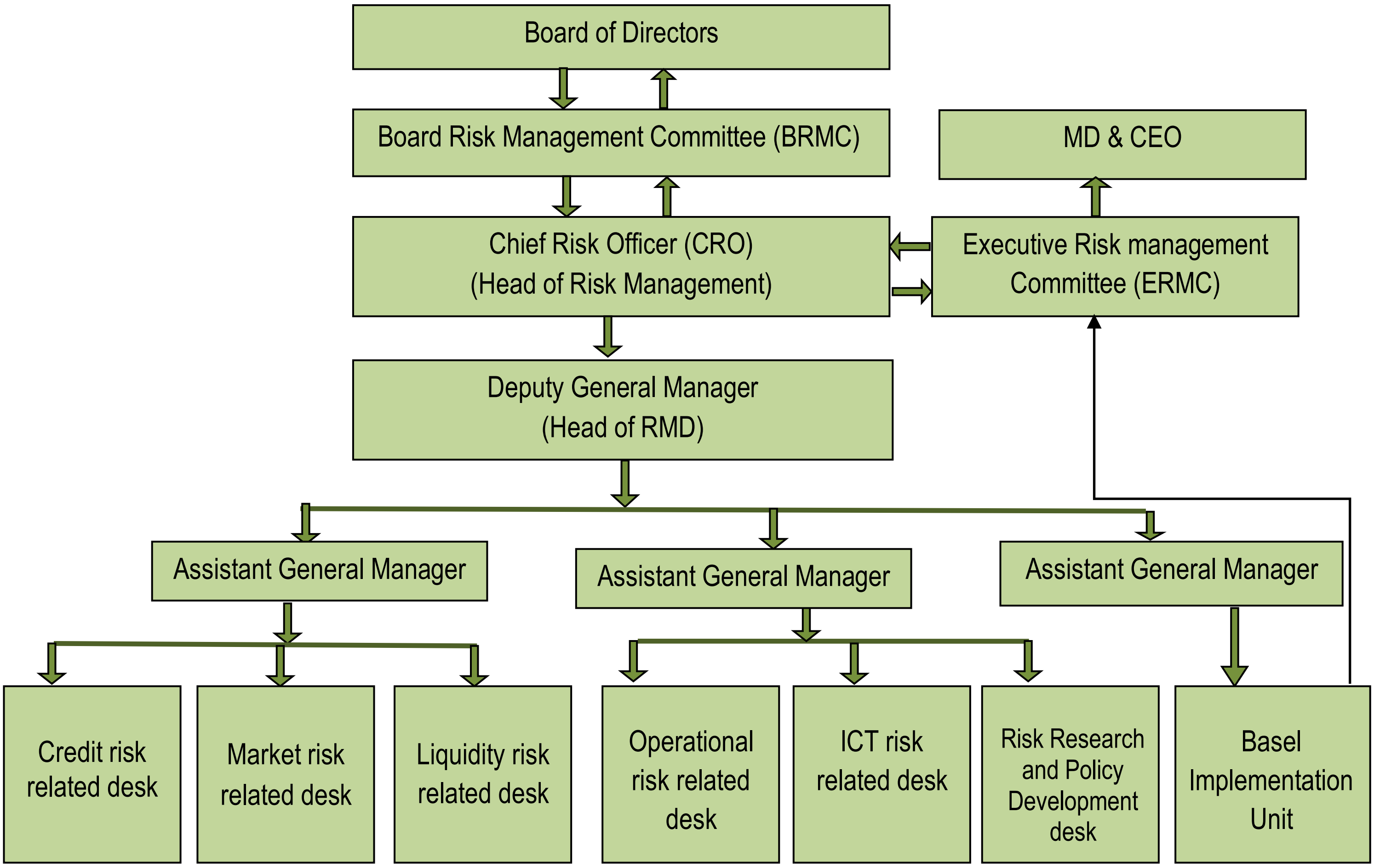
iv) Adequate documentation of coverage, procedures, findings and management responses to audits;

v) Appropriate and timely attention to identified material weaknesses and objective verification and review of management's actions to correct those deficiencies.

vi) Review of internal control information system

2.7 Risk Management Organogram

As per Bangladesh Bank's instructions vide circular letter no: 13 Date: 09-09-2015, ABL has already established an organizational structure for risk management division headed by DMD as Chief Risk Officer (CRO) and a General Manager in charge of Risk management. Besides there is a Risk Management Committee at board level developed in line with BB instructions in this connection. Risk Management organ gram of ABL is as follows:



2.7.1 Role of Board of Directors

The Board of Directors of the Bank shall give utmost importance on sound risk management practices and take every possible initiative to keep various risks (credit, market, liquidity, operational risks etc.) within tolerable level. Role of the board includes the following:-

a) Establishing organizational structure for risk management within the bank and ensuring that management as well as staffs responsible for risk management possess 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 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 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) Monitoring implementation of risk management policies & process to ensure effective prevention and control measures;

Policies/Guidelines/Manuals approved by the Board and presented through the Risk Management Committee:

As per Bangladesh Bank Guidelines on Core Risk Management, Bank has developed six core risk management guidelines in line with the core risk Guidelines of Bangladesh Bank. These guidelines are subject to review by the Board at least once in a year. Bank has six core risk management guidelines in place:

- Credit Risk Management
- Asset Liability Risk Management
- Foreign Exchange Risk Management
- Money Laundering Risk Management
- Internal Control & Compliance Risk Management
- Information & Communication Technology (ICT) Risk Management

These policies/guidelines of the bank are reviewed time to time in accordance with Bangladesh bank instructions. The contents, concerned authorities and latest revision updates of these core risk guidelines have been discussed below in brief:

Credit Risk Management Guidelines: The major contents/aspects/issues incorporated in Credit risk management Guidelines of the bank are as follows:

- Credit Risk Management
- Policy Guideline of CRM
  - ✓ Lending Guideline
  - ✓ Credit assessment of risk grading
  - ✓ Approval Authority
  - ✓ Internal Authority
- Organizational Structure
  - ✓ Preferred Organizational structure
  - ✓ Impose responsibility of individual officer

- Procedural Guideline
  - Approval process
  - Credit Administration
  - Credit monitoring
  - Credit recovery
- Lending Guideline
  - Industry/Business focus
  - Type of loan facility
  - Lending cap
  - Single borrower facility
  - Loan Appetite

- Organizing Credit Risk Management
  - Role of Board
  - Role of Senior Management
  - Role and responsibilities of CRECOM (Credit Committee)
- Credit Concentration
- Risk Appetite
- Credit Risk Mitigation Strategies
- Managing Credit Risk in the origination Process
- Managing Credit Risk in the Administration Process
- Managing Credit Risk with Appropriate Management Information Systems (MIS)
- Managing Credit Risk of Problem Assets
- Roles and Responsibilities of Credit Officers & Staff

The Credit risk management guidelines is prepared and revised by the Credit Policy and Credit Risk Management Division (CPCRMD) of the bank in line with the Guidelines on Credit Risk Management (CRM) for Banks given by Bangladesh Bank

Asset Liability Risk Management policy: The major contents/aspects/issues incorporated in Asset Liability Management (ALM) policy of the bank are as follows:

- Basel III Liquidity Ratios
  - Liquidity Coverage Ratio (LCR)
  - Net Stable Funding Ratio (NSFR)
  - Leverage Ratio
  - Advance to Deposit Ratio (ADR)
  - Wholesale Borrowing Guidelines (WBG)
  - Commitments
  - Structural Liquidity Profile (SLP)
  - Interest Rate Risk Management
  - Swapped Funds Limit
  - Contingency Funding Plan (CFP)

- Organizational structure of ALCO (Asset Liability Committee)
- Role of Treasury
- The ALCO process (Meeting of the committee, ALCO Paper, Market Risk, Liquidity Risk, Responsibility of related divisions)

The Asset Liability Risk Management policy of the bank is prepared and revised by the Treasury Division of the bank in line with the Asset Liability Management (ALM) Guidelines given by Bangladesh Bank.

Foreign Exchange Risk Management Manual

The major contents/aspects/issues incorporated in Foreign Exchange Risk Management manual of the Bank are as follows:

- ✓ Introduction
- ✓ Functions and Organizational set up of Agrani Bank Limited
- ✓ Functions of Treasury Front Office (Under Treasury Division)
- ✓ Functions of Treasury Mid Office (Under IT&FCMD)
- ✓ Functions of Treasury Back Office (Under IT&FCMD)
- ✓ Organization setup
- ✓ Dealing Room
- ✓ Counterparty Limits
- ✓ Triggers
- ✓ Stop-Loss Order
- ✓ Dealing Limits
- ✓ Code of Conduct of The Foreign Exchange Dealers
- ✓ Risk Limit Management
- ✓ Value at Risk Limit
- ✓ Compliance with Foreign Exchange Regulations
- ✓ Risk Associated with Foreign Exchange Operations
- ✓ Treasury Activities
- ✓ Derivatives Guideline
- ✓ Risk Management Aspects in Derivatives and new product transactions
- ✓ Product Guidelines
    - Spot Foreign Exchange
    - Forward Foreign Exchange
    - Forex Options
    - Forex Swaps
    - Cross Currency Swap
    - Interest Rate Swaps

The Foreign Exchange Risk Management manual of the bank is prepared and revised by the Foreign Currency Management Division (FCMD) of the bank in line with the Core Risk Management in Banking: Foreign Exchange Risk Management given by Bangladesh Bank in this connection from time to time.

Internal Control and Compliance (ICC) Policy & Procedures ((1) ICC Manual (2) Internal Audit Manual (3) Risk Based Internal Audit Manual (4) Audit Compliance Manual (5) Audit Monitoring & Controlling Manual (6) IT Audit Manual)

The major contents/aspects/issues incorporated in Internal Control & Compliance policy & procedures of the Bank are as follows:

- Policy Guideline and Responsibilities
- Policy Guide line for Internal Control
- ICC Related Issues
    - ✓ The Organizational Structure of ICC
    - ✓ Standards of the Best Professional Practices
    - ✓ Core Risks Management
    - ✓ Special Board Meeting On Compliance Of Annual Inspection Report Of Bangladesh Bank
- Internal Audit Charter
    - Role and Responsibilities of Internal Auditors
    - Auditors' Ethics & Qualification
- Internal Audit Manual
- Internal Audit
- External audit
- Concurrent Audit
- Audit Procedures
    - ✓ Risk Based Internal Audit
    - ✓ Categories of Audit Findings
- Information Technology (IT) Audit Manual
- Inspection Manual (Inspection by the Controlling Office)
- Audit Monitoring and Controlling Manual
- Audit Compliance Manual

The Internal Control & Compliance policy & procedures of the bank is prepared and revised by the GM Secretariat, Internal Control & Compliance (ICC) and Audit Monitoring Division of the bank in line with the Guidelines on Internal Control & Compliance in banks given by Bangladesh Bank.

Information & Communication Technology Security Policy

The major contents/aspects/issues incorporated in Information & Communication Technology security policy are as follows:

- ICT security management
- ICT risk governance
- ICT risk assessment
- Problem management
- Capacity management
- Server security controls
- Data center controls
- Networks security management
- Internet access management
- User access management
- Physical security for abl premise
- Working outside designated office hours
- Physical entry controls for visitors guests
- Business continuity plan (bcp)
- Disaster recovery plan (drp)
- Data backup and restore management
- Vendor selection for system acquisition
- In-house software development policy
- Software documentation
- Statutory requirements
- ATM/pos transactions
- internet banking
- payment cards
- SMS banking

The Information & Communication Technology Security policy is prepared and revised by the Information Technology & MIS (IT&MIS) Division of the bank in line with the Guideline on ICT Security For Banks and Non-Bank Financial Institutions given by Bangladesh Bank in this connection from time to time.

Money Laundering & Terrorist Financing Risk Management Guidelines: The major contents/aspects/issues incorporated in Money Laundering & Terrorist Financing Risk Management Guidelines are as follows:

- Money Laundering Operations
- Requirements of the Act
- Organizational Structure
- Procedures and Processes
- KYC Profile Form
- Transaction Profile Form
- Suspicious Transaction Reporting Form
- KYC Implementation Plan for Existing Accounts

The Money Laundering & Terrorist Financing Risk Management Guidelines of the bank is prepared and revised by the Money Laundering & Combating Terrorist Financing Division of the bank in line with the guidelines on Money Laundering & Terrorist Financing Risk Management Guidelines given by Bangladesh Bank in this connection from time to time.

Strategies and activities of BRMC in overseeing risk management functions of the bank:

- **Annual Business Targets and achievement:** Bank formulates an annual Business targets at the beginning of each year. The business targets are estimated by the approval of the board and used for performance appraisal of employees based on achievement of target. Annual Business targets are set by the Planning, Co-ordination and marketing Division (PCMD) of the Bank.

- Risk Management Committee Review and propose the setting of the risk appetite/tolerance of the Bank to the Board. The Risk Appetite is reviewed and compared with the performance of the bank time to time

- Risk Management reporting and compliance that BRMC looks into for decision making on risk management of the bank are as follows:

  - ✓ Review of CAMELs rating of the bank (provided by BB twice in a year in June and in December);
  - ✓ Review of CRMR (Comprehensive Risk Management Reporting) rating of the bank (provided by BB twice in a year in June and December)
  - ✓ Review of decisions taken at the ERMC (Executive Risk Management Committee) in monthly meeting
  - ✓ Capital position of the bank
  - ✓ Scenario of Stress Testing

- ✓ Compare actual situation of different risk areas with Risk Appetite/limit set by the Board
- ✓ Findings on risk Management reporting of MRMR (Monthly Risk Management Report) and CRMR (Comprehensive Risk Management Report) prepared on monthly and half yearly basis in format of BB
- ✓ Review of observations and recommendations of BB given in Core Risk Inspection report/CRMR Rating/CAMELs Rating
- ✓ Review of Bank's entity Credit rating performed by ECAI (presently credit rating is performed by Alpha credit rating)

❖ **Loan Recovery Strategy:** Strategy initiated for recovery against NPLs. The recovery strategy is prepared and reviewed by RNPAMD (Recovery & NPA management Division Recovery). RNPAMD holds meeting at NPLMC (NPL Management Committee) to oversee recovery progress and submits follow up report on the recovery against large loan in BRMC.

b) Ensuring construction of adequate organizational structure for managing risks within the bank;

c) Supervising the activities of Executive Risk Management Committee (ERMC) ;

d) Ensuring compliance of BB instructions regarding implementation of core risk management;

e) Ensuring formulation and review of risk appetite, limits and recommending these to Board of Directors for review and approval;

f) Holding at least 4 meetings in a year (preferably one meeting in every quarter) and more if deemed necessary;

g) 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;

h) Complying with instructions issued from time to time by the regulatory body;

i) Ensuring appropriate knowledge, experience, and expertise of lower-level managers and staff involved in risk management;

j) Ensuring sufficient & efficient staff resources for RMD;

k) Assessing overall effectiveness of risk management functions on yearly basis.

l) Establishing standard of ethics & integrity for staff and enforcing these standards

2.7.3 Role of Executive Risk Management Committee (ERMC)

Bank has formed ERMC comprising of CRO (as the head of the Committee) and the Heads of ICC (Internal Control & Compliance), CPCRMD (Credit Policy & Credit Risk Management), Treasury & ID (International Division), AML (Anti Money Laundering), ICT, accounts (CFO-Chief Financial Officer), Recovery and any other department related to risk. RMD shall act as secretariat of the committee. The ERMC may invite top management (MD & CEO, DMD or other senior executives), to attend the meetings so that they are well aware of risk management process.

The responsibilities/ Terms of Reference of ERMC include, but not 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;

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 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) Following up reviews and reports from BB and informing BRMC the issues affecting the bank's operation.

l) Taking initiative to arrange risk conference/open discussion session annually to create risk awareness and learning across the bank.

2.7.4 Chief Risk Officer (CRO)

Chief Risk Officer (CRO) is responsible for ensuring intense and effective risk management across the bank. The CRO ensures 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. Appointment, dismissal and other changes to the CRO position should be approved by the board or its risk management committee. The removal of CRO should be disclosed publicly accompanied by the reasons for such removal. CRO's performance and compensation shall be reviewed and approved by the board or Board Risk Management Committee.

Criteria 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 shall be equal to or at-least one grade higher (i.e. at least a General Manager) than the other department heads for effective risk management.

2.7.4.2 Role of Chief Risk Officer (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 it's Risk

Management Committee. He or she is to be directly supervised by the Board Risk Management Committee (BRMC).

CRO shall not have any reporting relationships with business verticals of the bank and 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 MD & CEO for acknowledgement. The CRO will have access to any information necessary for performing duties. In this context board and MD& CEO will provide full support to him/her. CRO shall undertake the following responsibilities 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 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 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 global economic and financial positions;
- To include risk aspects in Annual Conference with the participation of all the 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, and Chief of the internal audit function or any other function.

2.7.5 Risk Management Division (RMD)

Bank must have an independent full-fledged Risk Management Division. The Risk Management Division shall be headed by the Chief Risk Officer (CRO) and structured with separate desks for overseeing each key risk area.

The main functions of the department include, but not limited to, the following:

- Managing the process for developing risk policies and procedures;

- ❑ Coordinating with different operational units to prepare task specifications;

- ❑ Preparing and forwarding risk reports to both internal and external authorities ; and

- ❑ Assisting in the implementation of all aspects of the risk function.

The risk management functions are functionally and hierarchically independent from business and other operation functions. The officials dealing with risks shall not be given responsibility for monitoring and evaluating their risks and equipped with sufficient resources and personnel should possess needed experience and qualifications.

According to BB instructions, 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's risk, i.e. when the capital increases, the bank risk decreases. Hence, a close relationship and communication shall exist 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 ;

- ❑ 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 ALCO, NPLMC, Credit Committee, Management 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 Risk Management Division (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 following:

- 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 highlighting the risk management practices, risk management present and future work plan;
- Establishing sophisticated risk management infrastructure and developing a bank wide 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 VaR (Value at Risk) model for market risk analysis;
- 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 risk governance framework which includes the bank's risk culture, risk appetite, risk limits;
- Monitoring 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 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 (shifting risk to others through insurance coverage), risk avoidance and risk retention program
- Taking appropriate steps to control or mitigate risk exposures and ensure reporting the same to senior management and BRMC.
- RMD will prepare a comparative analysis report on bank's gain/loss due to/lack of proper risk management activities and its impact on capital and produce 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 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 divisions. Specific tasks of different RMD desks:

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 (Management Action Trigger) 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 exposure, forced loan, movement of adverse classification, collateral against loans, credit rating of borrowers, taken over loans etc.;
- 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, 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 advising 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.

<u>Risk Research and Policy Development desk</u>

- Developing, testing, and using different models such as VaR 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 Concept of Risk Appetite

The risk management framework 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 contain strategic planning of the bank including regulatory requirements and legal obligations.

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

Information to be incorporated in a strategic plan are outlined below:

a) Analysis of the external environment in which the bank operates;

b) 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) Reducing Non-performing loans

h) Increasing NPL recovery

i) Deposit growth with a view to optimizing cost of fund

j) Lending growth with industry and business segment focus

k) Maintaining adequate capital for absorbing all material losses

l) Maintaining optimum liquidity

m) Risk Appetite Statement for all material risks

n) Automation and effective Management Information System (MIS)

o) Proactive risk management and governance

2.8.1 Definition of Risk Appetite

Risk appetite is the aggregate level and types of risk a bank is able and willing to assume within its risk capacity and risk/return attributes to achieve its strategic plan preserving the interest of stakeholders i.e. depositors, creditors, borrowers, regulators etc. A well documented, operational and clearly defined risk appetite provides the bank with a framework that facilitates management to be informed and confident in taking appropriate levels of risks. Risk appetite can be expressed through quantitative and qualitative means considering the extreme conditions, events and outcomes in terms of the potential impact on profitability, capital and liquidity.

2.8.2 Objectives of Risk Appetite

- Developing risk portfolio views;
- Monitoring and reporting risk profile;
- Controlling and correcting risk profile;
- Determining, calculating and articulating risk tolerance/risk threshold;
- Aligning the risk profile to the business plan and capital management plan;
- Upholding the highest ethical standards of conduct;
- Preserving the long-term financial resilience of the bank;
- Avoiding losses when investing money;
- Ensuring compliance with legal and regulatory obligations; and
- Maintaining a robust internal control environment and safeguarding operational continuity.

2.8.3 Risk Appetite framework

Risk appetite framework is the overall approach together with policies, processes, controls, and systems through which risk appetite is established, communicated, and monitored. It includes a risk appetite statement, risk thresholds and limits, and an outline of the roles and responsibilities of those overseeing the implementation and monitoring the risk appetite framework.

2.8.3.1 Element of Risk Appetite Framework

Risk appetite is the cornerstone of a successful risk management framework. Risk appetite can be fitted into the risk management framework in the following manner:

- **Risk governance**: Clear risk appetite approved by board, embodied in risk policy and delegated authorities. This sets 'tone from the top' and a foundation for the risk culture.

- **Risk assessment**: Frequent risk assessment process to identify new and changing risk landscape in context of risk appetite.

- **Risk quantification and aggregation**: Regular quantification and aggregation of risk to priorities focus of risk management and control.

- **Monitoring and reporting**: Monitoring and reporting of performance against risk based limits based on risk appetite.

- **Risk and control optimization**: Framework of controls calibrated in line with risk appetite to optimize cost/benefit.

2.8.3.2 Effective Risk Appetite Framework (RAF)

Some fundamentals for an effective RAF are mentioned below:

- Being reviewed and approved by the board at least annually;
- Making forward-looking discussions of risk easier;
- Being consistent with the bank's strategy, objectives and stakeholders' demands, key strengths and competitive advantages;
- Discussing the desired business mix and composition of the balance sheet, risk preferences, tolerances for volatility, capital thresholds, tolerance for post-stress loss, optimum liquidity ratios etc.;
- Engaging the board/management in developing/implementing a risk-conscious strategy and in capital planning and allocation;
- Being the ability to measure, monitor, and adjust as necessary the actual risk positions against the established RAP for addressing all material risks;
- Recognizing losses thus setting loss tolerances that are reflective of overall business objectives;
- Reflecting the human and technological resources needed to measure and manage the bank's risks in a timely fashion;
- Having a formal and transparent governance structure that clears roles for all internal stakeholders;
- Documenting risks as part of a risk register, including risk-specific definitions, how often each risk will be measured, assumptions related to each risk, judgment on severity and likelihood, and speed at which risks could manifest.

2.8.4 Risk Appetite Statement

Risk appetite statement is a formal statement in which the management expresses its views on the amounts and types of risk that the bank is willing to take in order to meet its strategic objectives. It includes qualitative statements as well as quantitative measures expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate.

2.8.4.1 Steps for 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:

- ❑ Analysis of the growth, prospect, long-term plan of national economy;
- ❑ Study of the concentration, growth, NPL, profitability, capital, liquidity etc. of banking industry and peer group;
- ❑ Considering the national thrust, regulatory requirements etc.;
- ❑ Considering bank's own portfolio growth, trend of NPL, profitability and capital, liquidity position, risk management culture and practices etc;
- ❑ Considering the bank's overall strategic and financial objectives;
- ❑ Determine the bank's risk profile;
- ❑ Setting tolerances for exposures and potential losses in consultation with the business line and related departments;
- ❑ Getting board approval and communicating it throughout the bank.

2.8.5 Areas of Risk Appetite

Bank prepares risk appetite statement covering regulatory requirements related to all material risks, components of pillar II under Basel III, strategic planning and all other probable risks exist in the bank. Bank sets risk appetite, tolerance and limit for all the probable areas of risks. Some possible areas for setting risk appetite are as follows:

Loan concentration (sector/industry/geographical area/borrower-wise);

- ❑ Overall growth of total loans and advances including off-balance sheet items;
- ❑ Gross and net NPL to total loans;
- ❑ Cash recovery against classified loan/written off loan;
- ❑ loan outstanding with acceptable rated customers;
- ❑ Unsecured exposure to total exposure (funded);
- ❑ Rescheduled loans to total classified loans
- ❑ Written off loan to total classified loans
- ❑ Interest waiver as a percentage of NPL;
- ❑ Bucket-wise gap under simple sensitivity analysis for interest rate change;
- ❑ Liability concentration (Top-10 deposit suppliers to total deposit);
- ❑ Bucket-wise gap under structural liquidity profile (SLP);
- ❑ Expected loss from operational risk;
- ❑ Operating expenses to operating income; and
- ❑ Various ratios (ADR) etc

RISK MANAGEMENT PROCESS

3.1 Risk Management Process

Considering the complexity, size and nature of business, risk strategy, ABL has developed and implemented risk management guidelines which comply with the latest core risk guidelines and risk circulated by BB for effective risk management.

ABL also considers bank's capital adequacy, expected level of profitability, market reputation, adequacy and HR expertise, logistic support, macro and micro economic scenario, risk management practices etc. to determine the risk strategy.

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: Risk Management must be performed following few steps one by one which have been outlined and described below**:**

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

The risk initiatives, monitoring tools, reporting and mitigation techniques that are detected and produced in different reporting formats are needs to be disseminated to different operational layers for mitigation of risks and implementation of decisions in this regard taken by management and board. This step includes the following:

- Management communicate the roles, responsibilities, accountabilities of the internal stake holders (employees, management, board) ;
- Formation of policies, review/revision, and dissemination of the policies;

- Risk owners/originators (The operational unit where the risk evolves) are informed of his/her/their role when dealing with the risks;
- All the stake holders are communicated after due consultation that everybody informs 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 preferably required to 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:

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

a) <u>Establish the internal context</u>:

In ABL, Changes in internal policies, operational dimensions, adoption of ICT, changes in strategy etc. are considered in risk management process. This ensures that risk decisions always support the broader goals and objectives of the business. This approach encourages long-term and strategic thinking.

b) <u>Establish the external context</u>

This step defines the overall environment in which the bank operates. It is an analysis to identify the strengths, weaknesses, opportunities and threats to the business in the external environment by means of industry analysis in performance, quality of service, different risk indicators that can be measured quantitatively and qualitatively. In addition to the local issues ABL shall also consider Local and global issues related to risks so that it can minimize the risk areas within the regulatory framework and ensure a strong and effective risk management.

c) <u>Establish the risk management context</u>

ABL defines, detects and measures the limits, objectives, appetite and scope of the activity or issue in conducting a risk analysis for a new product or project loan, introduction of a new branch, or a new product line through the marketing and Development Division (PCMD) 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 it occurring.

Bank identifies risks by the following two ways:-

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 (Internal, Commercial and External)
- ❑ Various risk reports (MRMR, CRMR, CAMELs, Core risk inspections reports, large loan concentration, capital Adequacy, rescheduled loans etc.)
- ❑ Regular reports (Recovery, write off, law suits, overdue bills, profitability, earnings capacity etc)
- ❑ Hazard or incident logs or registers (Any unforeseen event in any operational activity should be brought under consideration)
- ❑ Customer complaints (Received directly at head office and in customer complaint box of branches)
- ❑ Changes in regulations (Any change in regulatory limit, policies, requirements, reporting format, rules etc)
- ❑ Media reports (Print or electronic)

❑ Bangladesh Bank inspection report (core risk, branch, head office, divisional inspections)

2. Identifying prospective risks:

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

Methods for identifying prospective risks include:

- ❑ Regular view exchange with staff as well as external stakeholders like depositors, creditors, borrowers, regulators, Government officials

- Researching the economic scenario to get a comprehensive idea relating to different risk parameters, risk areas, risk management as well as mitigation technique, policies and in macro or micro level in both local and global arena.

- Conducting interviews with the relevant people and/or organizations to get a clear risk management idea from the operational layer where risk originates form, it is essential to take the key personnel or key risk zones/areas or key risk parameters into consideration so that risks are well understood, managed and mitigated effectively.

- Undertaking surveys of staff or clients to identify anticipated issues or problems or risks: It is natural that the person dealing with a risk understands the nature, complexity, severity, frequency or materiality of risk/s. In this context, staffs should be consulted or even given a space in decision making or consultation process for effective management of risks at enterprise level.

- Reviewing policy, process, systems at least once a year or even based on economic scenario at micro or macro level changes in local and global economic condition, industry practice, banking functions etc.

Step 4. Analysis of the risks

The risk analysis assists in determining which risks have a greater consequence or impact than others. Thus analyzing the likelihood (possibilities of happening of risk/s) and consequences (Outcomes/implications/results/damages/loss) of each identified risk and deciding which risk factors will potentially have the greatest effect and should, therefore, receive priority with regard to how they will be managed.

The level of risk is analyzed by combining estimates of likelihood in different scenario (table 1) and consequences in different magnitude (table 2). Based on the severity and the frequency of risk parameters, scale can be determined from the scale shown in the tables:

Table 3.1– Likelihood scale

Rating	LIKELIHOOD
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 3.2 – Loss or damage impact scale

Rating	POTENTIAL IMPACT
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

The scaling shall be performed from the operational layer where risks are originated from and compiled at head office level to see the picture in entire bank. The output of the analysis can be used in the annual risk reports and place before ERMC, BRMC and Board for recommendations and further proceedings.

Step 5. <u>Evaluation of the risks</u>

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. Management, BRMC and Board will see the likeliness of the risks along with the severity and consequences as set in the business strategy, risk appetite and internal limits and any breach of actual estimates lead to further revision of the activities or the risk mitigation techniques.

Step 6. <u>Treatment of risks</u>

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. This will enable bank management and the board to decide whether to accept such risks in future or to avoid/ignore/shift /transfer the risks by means of a change in strategic choice.

<u>Options for risk treatment</u>

Identifying options from the following in the minimization of negative risk or an increase in the impact of positive risk.

1. Avoid the risk (Avoid or ignore the issues that create risks)
2. Change the likelihood of the occurrence (Take initiative to change the frequency, possibility of occurrence so that risk can be minimized)
3. Change the consequences (Make an estimate of plausible loss to be absorbed in such a way that causes the minimum or reasonable damage in case of the happenings of the risk indicator/parameter)

4. Share the risk (Take proper risk coverage techniques like insurance, offset the risk with non-risk indicators, diversify risks through the different dimensions at enterprise level).
5. Retain/Accept the risk supported by the CRAR as per Basel III (Verify the strength of existing capital base whether or not satisfactory to address the accepted level and the consequences of risk. In case of situation where bank maintains a substantial amount and percentage of capital/CRAR above the minimum required level, bank may think of accepting further risk in consideration of the resilience of bank in terms of capital support and financial strength)

Following are the options that can be applied individually or in combination to address risks:

- ❑ 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. It is natural that 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. Risk management plan shall 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.

3.3 KRI/Risk Register:

Bank should maintain KRI as one of the effective tools for comprehensive risk management 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.

Operational managers at branch, zones and circle shall report the key risks issues to RMD as and when identified/detected. RMD will act as second level of defense and 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 (Board Risk Management Committee) on quarterly basis.

Minimum components of risk register include the following:

- ✓ **Date:** record risk identification date, target date and completion dates for treating risks.
- ✓ **Risk Number**: A unique identifying number of the risk
- ✓ **Risk Description**: A brief description of the risk, it's causes and impact
- ✓ **Existing Controls**: A brief description of the controls that are currently in place for the risk
- ✓ **Consequence**: The consequence (severity or impact) of rating for the risk, using scales(e.g. 1-5 with 5 being most severe)
- ✓ **Likelihood:** The likelihood(probability) rating for the risk, using scales (e.g. 1-5, with 5 being most likely)
- ✓ **Overall risk score:** Determined by multiplying likelihood (probability) times consequence (Impact) for a scale ranging from 1-25
- ✓ **Risk Ranking**: A priority list which is determined by the relative ranking of the risk by their overall risk score
- ✓ **Trigger**: Something which indicates that a risk is about to occur or has already occurred
- ✓ **Management Action**: Action which is to be taken if the risk found adverse
- ✓ **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, bank follows latest core risk management guidelines/policies/manuals of the bank on Credit, Foreign Exchange, Asset-Liability (including appendix), Internal Control & Compliance, ICT security and Prevention of money laundering and terrorist financing prepared in line with the respective guidelines issued from BB.

Bank has also developed different tools and models for measuring credit, market and liquidity risks. For example: Interest rate sensitivity and duration analysis for interest rate risk, Stress testing for credit, market and liquidity risk, structural liquidity profile for liquidity risk etc.

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, but exists in the natural course of corporate activity, and 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.

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. This may arise from uses people, process, and technology to achieve business plans. 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.

4.2 Categorization of operational risk

Agrani Bank limited, being one of the largest banks in terms of geographical network, has made the following categorizations of operational risk events, according to Event Type and operational strata.

Event Type	Business Line	Scenario Descriptions
Type A: Internal Fraud	Applicable for all operational layers / Business Line and for all the functions performed by the bank including the functions under general Banking, Credit management, Foreign Exchange, Agency services, reporting and compliance etc **(All Circles, zones, branches, head Office, Controlling Office, Subsidiaries)**	a) Loan Fraud b) Embezzlement c) Failure to follow procedures/limits d) Theft of customer data/information e) Misappropriation of assets f) Theft of assets g) Fraudulent transfer of funds h) Theft of customer funds
Type B: External Fraud	Applicable for all operational layers / Business Line and for all the functions performed by the bank including the functions under general Banking, Credit management, Foreign Exchange, Agency services, reporting and compliance etc **(All Circles, zones, branches, head Office, Controlling Office, Subsidiaries)**	a) Client misrepresentation of information b) Theft c) Loan fraud d) Cybercrime d) Forgery e) Cheque fraud f) Theft of information/data g) Fraudulent transfer of funds h) Credit product fraud (loans, L/C, guarantees) i) Payment fraud j) Robbery
Type C: Employment Practices and Workplace Safety	Applicable for all operational layers / Business Line and for all the functions performed by the bank including the functions under general Banking, Credit management, Foreign Exchange, Agency services, reporting and compliance etc **(All Circles, zones, branches, head Office, Controlling Office, Subsidiaries)**	a) Discrimination b) Occupational accident c) Discrimination d) Environmental issue e) Wrongful termination etc

Type D: Clients, Products, and Business Practices	Applicable for all operational layers / Business Line and for all the functions performed by the bank including the functions under general Banking, Credit management, Foreign Exchange, Agency services, reporting and compliance etc **(All Circles, zones, branches, head Office, Controlling Office, Subsidiaries)**	a) Regulatory breach b) Compromised customer information c) Fiduciary breach d) Compromised customer information e) Noncompliance with money laundering f) Mis-selling g) Client suitability
Type E: Damage to Physical Assets	Applicable for all operational layers / Business Line and for all the functions performed by the bank including the functions under general Banking, Credit management, Foreign Exchange, Agency services, reporting and compliance etc **(All Circles, zones, branches, head Office, Controlling Office, Subsidiaries)**	a) Business continuity failure b) Damage to building and premises c) Fire d) Flood e) Natural disaster f) Terrorist attack g) Vandalism h) Earthquake
Type F: Business Disruption and System Failure	Applicable for all operational layers / Business Line and for all the functions performed by the bank including the functions under general Banking, Credit management, Foreign Exchange, Agency services, reporting and compliance etc **(All Circles, zones, branches, head Office, Controlling Office, Subsidiaries)**	a) IT system failure b) Utility outage c) Off-shoring/Outsourcing risk d) Failure of payments infrastructure

Type G: Execution, Delivery, and Process Management	Applicable for all operational layers / Business Line and for all the functions performed by the bank including the functions under general Banking, Credit management, Foreign Exchange, Agency services, reporting and compliance etc **(All Circles, zones, branches, head Office, Controlling Office, Subsidiaries)**	a) Inaccurate/Incomplete contract b) Transaction error c) Staff error in lending process d) Data entry error e) Model risk f) Pricing error g) Failure of external supplier h) Failure to follow procedures i) Lost or incomplete loan/legal documentation j) Processing error k) Collateral management error l) Mismanagement of account assets m) Unapproved access given to client accounts n) Inaccurate financial statement o) Failure of supplier/vendor Tax noncompliance

4.3 Operational risk management framework

Operational risk management framework articulates operational risk issues in the bank and covers the bank's tolerance for operational risks. Operational risk management frameworks in bank are guided by the following:

- Risk management Guidelines for banks issued by BB and banks internal risk management guidelines
- Circulars/Instruction/policies/manuals, guidelines issued from BB or by the bank that covers the operational risk management functions like Core risk management guidelines for Credit risk management, Asset Liability management, Foreign Exchange risk management, Internal Control & Compliance risk management, Money Laundering risk management, Information & Communication & Technology risk management, Guidelines on risk based capital Adequacy for banks, Stress testing guidelines for banks, all other prudential guidelines that falls under operational risk management of the bank, HR policy of the bank, all other related circulars that considers and include the scope of operational risk management.

ABL has no separate operational risk management wing rather it is performed as a part of the entire risk management of the bank under Risk management division by means of reporting to internal and external authorities and regulatory compliance. The bank's operational risk management framework is commensurate with the bank's risk profile. The framework also articulates the key processes the bank needs to have in place to manage operational risk. Besides Frauds, forgeries, embezzlement etc are being detected, Verified and settled by separate divisions under different operational layer at field and head office level:

a) Audit & Inspection Division
b) Vigilance Division and
c) Zonal Offices and Circle offices etc

4.4 Board oversight

The board oversees the operational risks by delegating authority in different layers under the direct supervision of top management through MANCOM, ALCOM, and CRECOM etc. To make Operational risk management most effective, bank emphasizes in establishing high standards of ethical behavior at all levels of the bank. The board also promotes an organizational culture by means of policies, procedures, rules, regulations etc (HR policies, Core risk policies, internally generated circulars and instruction letters, BB circulars), 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 under Risk Appetite statement and set strategic direction in relation to operational risk;

b) Approve the implementation framework designed to explicitly manage operational risk for 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 management structure (divisions like BSUCD, PCMD, HRDGA, HRPDOD, ICC in head office as controlling body) 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 aspects 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 different policies, processes and procedures to be implemented;

b) Clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability and ensure that the necessary resources are available to manage operational risk;

c) Ensure that bank activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources, and that staff responsible for monitoring and enforcing compliance with the bank's risk policy have authority and are independent from the units they oversee;

d) Ensure that the bank's operational risk management policy has been clearly communicated to staff at all levels of the organization that are exposed to material operational risks.

4.6 Policies, procedures and limits

The operational risk management policy of the bank include at least, but not limited to, the followings:

- ❑ The strategy given by the board of the bank for operational risk management by setting targets, policies, rules;
- ❑ The systems and procedures incorporated for effective operational risk management and
- ❑ The structure of operational risk management function and the roles and responsibilities of individuals involved
- ❑ The policy includes any new or changed activity such as new products or systems conversions is evaluated for operational risk by respective divisions/ units prior to coming into effect and such activity must be approved by the board and documented.

- Bank has documented policies along with a ToR (Terms of References) regarding scope and functions of the outsourcing activities (like online support, technical assistance, software supply & installation etc) and has written policies for managing the risks associated with outsourcing activities. Use of third parties needs to be ratified by 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 are made 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, bank considers risks associated with outsourcing arrangements, including disruption of services.

4.7 Risk assessment and quantification

Bank assesses the operational risk inherent in all material products, activities, processes and systems and its vulnerability to these risks. Bank 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 by respective divisions/units concerned with the origination**.**

Tools that used by bank for identifying and assessing operational risk are:

(a) **Self risk assessment:** bank uses internally as well as externally approved reporting format to identify the strengths and weaknesses of the operational risk environment.

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

(c) **Risk indicators**: bank uses several risk indicators, often financial, to get an insight into a bank’s risk position. These indicators (staff turnover rates, the frequency and/or severity of errors and omissions. Threshold/limits set as part of Risk Appetite Statement) are subject to review on a periodic basis (such as monthly or quarterly) to alert bank to changes that may be indicative of risk concerns.

(d) **Historical data analysis:** Bank uses trend data to determine possible operational risk and developing a policy to mitigate/control the risk.

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 are used to reduce the exposure to, or frequency and/or severity of such events. Mitigation tools like insurance, back up, monitoring, control system are used for Losses of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

Information technology security is also important for risk mitigation. However, bank needs to be aware that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses caused by internal factors or by factors beyond the bank's immediate control e.g. external events. In this connection, Bank has in place the disaster recovery and business continuity plans to address this risk.

4.9 Risk monitoring

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. Considering such effects, bank performs regular reporting of pertinent information to senior management in different committee and to the board as well as board level committees to support the proactive management of operational risk. Besides, core risk areas are performed in accordance with the instructions included in the respective risk management policies of the bank. Besides, senior management ensures the following:

a) Monitor assessment of all types of operational risk faced by the bank through reporting and compliance on periodic frequency (Various reports are generated and reported to internal and external bodies in different frequencies);

b) Assess the quality and appropriateness of mitigating actions, review effectiveness of the same periodically in different meetings at board and management level; and

c) Ensure that adequate controls and systems are in place to identify and address problems before they become major concerns.

In addition to monitoring operational loss events, bank also specify and identify appropriate indicators such as rapid growth, the introduction of new products, employee turnover, system failure, and so on. Regular reviews are carried out by internal audit, or other external audit teams, to analyze the control environment and test the effectiveness of implemented controls, thereby ensuring business operations are conducted in a controlled manner.

Monitoring activities can be performed in three layers which can be categorized in the following way:

I) **Operational layer**: Operational level includes branches and zonal offices that faces the risk issues directly or where the risks originated from;

II) **Controlling layer**: Zonal Office and Circle office will monitor activities relating to risks in branch level;

III) **Strategic layer**: Top management including MD & CEO , DMDs, GMs and other controlling wing at head office level like ICC, MANCOM, ALCOM will oversee the functions of the previous two layers and make decisions accordingly

4.10 Risk reporting

Senior management ensures 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 includes 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 contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports are distributed to appropriate levels of management and to areas of the bank on which concerns may have an impact. To ensure the usefulness and reliability of these reports, management regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports.

4.11 Control mechanism

ABL has designed Control activities under direct supervision of ICC to address the operational risks identified. For all material operational risks that have been identified, the bank decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks based on the gravity of risks.

4.12 Contingency planning

Bank has 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 have been designed taking into account different types of scenarios to which the bank may be vulnerable. The Business continuity pan and disaster recovery plan 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.

4.13 Internal controls

Internal control system is established to ensure adequacy of the risk management framework and compliance with a documented set of internal policies concerning the risk management system. Major functions performed by internal control system include:

a) Review of the bank's progress towards the set objectives by top management on a regular frequency;

b) Checking compliance with management controls;

c) Policies, and procedures concerning the review, and resolution of non-compliance issues; and

d) System of documented approvals and authorizations to ensure accountability to the appropriate level of management.

Bank has 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 and risk management committee) ensure that the scope and frequency of the audit program is appropriate to the risk exposures. Audit team periodically validate that the bank's operational risk management framework is being implemented effectively across the bank.

CAPITAL MANAGEMENT

5.1 Relation between Capital Management & Risk Management

Capital management refers to implementing measures for maintaining adequate capital, assessing internal capital adequacy of the bank and calculating capital adequacy ratio in line with the guidelines on Risk based Capital Adequacy (revised regulatory framework in line with Basel-III) issued by Bangladesh bank vide circular No: 18 dated: 21 December 2014 .

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

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) under Pillar-II of basel-3, bank identifies the risks that the bank is exposed to (as per BB guidelines), 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 other mechanisms.

The outcomes of capital management are:

i. A Capital Plan highlighting the overall business performance of the bank including the capital position over a longer time horizon;

ii. Use of ICAAP (Internal Capital Adequacy Assessment Process) to determine additional or precise levels of required capital ;

iii. Regularly compare available capital with current and projected solvency needs, and address deficiencies in a timely manner.

5.2 Framework of Capital Management

Bank has established separate Basel implementation unit under Risk Management division for performing activities relating to capital management, to calculate the capital adequacy ratio and secure adequate capital to cover the risks it faces and to ensure soundness and appropriateness of the businesses. In this regard bank follows the latest guidelines on Risk Based Capital Adequacy and other related BB circulars/instructions to assess its capital adequacy.

For proper measurement and management of capital, bank has put in place strategy, decision making authority at the top including the board of directors, Executive Risk Management Committee and the top management. In this context, Roles and responsibilities as well as the framework of capital management can be outlined as below:

5.2.1 Roles and responsibilities of Board and Senior Management:

The Board and Senior Management shall act in the following way:

- ❑ **Capital management functions must include the following**:
  - ✓ Regulatory compliance so that capital levels always exceed or at least reaches BB's requirements;
  - ✓ Make sure Capital level is aligned with the risks in the business and consistent with the strategic plan, business plans, MOU ,APA etc.; and
  - ✓ Maintain capital at an appropriate level for protecting the interests of depositors and other creditors.
  - ✓ Calculation of the capital adequacy ratio in line with capital adequacy guidelines issued by Bangladesh Bank
  - ✓ Make sure Executive risk management committee discusses and suggests measures with regard to capital management in each monthly risk management committee meeting as well as in other committees
  - ✓ As per BB instructions, Basel Implementation Unit (BIU) has been set up with close relationship with RMD (as a separate unit), and in charge of the ICAAP and the calculation of the capital adequacy ratio has been kept independent from offices/divisions inside and outside RMD maintaining a check-and-balance system;

- Ensure consistency of the capital management system with the bank's risk profile and the competing business environment; Review capital ratios and levels of capital against the Bank's risk profile and risk appetite. Board must determine the satisfactory capital levels under specific stressed economic scenarios in consistent with the capital maintained, risk exposures, risk limit set under the Risk Appetite statement and make sure the capital remain above the regulatory and the internal requirements;

- 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, Incorporate an integrated capital management process into the bank's strategic plan for three-year time horizon along with two years previous data, considering key economic variables. 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 includes the following factors in setting the capital targets:

    - Regulatory capital requirements;
    - Expected asset growth and profitability;
    - Stress test scenarios.
    - Specifying the basis for the calculation of capital to be allocated to risk;
    - Preparing capital management rules specifying the arrangements appropriately based on the bank's business and risk profile;
    - Ensuring consistency of capital and the bank's corporate management policy and plans, its strategic objectives, etc.;
    - The basis for determining the capital as used in the regulations concerning capital adequacy ratios-Tier 1, Tier 2 capital, and eligible capital;

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).

Bank prepares Monthly Risk Management Report (MRMR) and Comprehensive Risk Management Report (CRMR) according to the formats provided by BB as a minimum requirement. Bank also includes additional information related to the concerned risk areas. Bank arranges monthly meeting of ERMC to discuss the risk issues based on the findings of the risk reports and 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 reflects in the meeting minutes. Bank also submits the board approved Risk Appetite Statement (RAS) on yearly basis and BRMC meeting minutes on regular basis. Besides Bank submits 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 sent to BB are signed by the CRO.

In addition, bank shall 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 Regulatory Penalty for non-compliance

If 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 bank fails to submit the above mentioned reports within stipulated time without any acceptable/satisfactory reason.

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 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 staff.