PAN ASIA BANK
The Truly Sri Lankan Bank

BANK WIDE
RISK MANAGEMENT POLICY

(For regulatory disclosure purpose)

SCOPE AND OBJECTIVE

1.1. Requirement for the policy

The Risk Management Policy of the bank has been designed to handle and mitigate the risks that prevail while carrying out the business of banking. This document will widely discuss and identify the risks faced in the functions of the bank and the requirement of the regulator to guide on the business of banking for the purpose of control and monitoring.

The policy considers the options of growth of business with reasonable risk exposures which do not hamper the return on such actions and keeping in line with the best practices of the industry. The level of competition, growth in technology and the changes in the communication industry will compel banks to spearhead their activities to meet the demands of new businesses and financial instruments. Relaxation of certain controls may pressurize banks to adopt their own controls to monitor the risks associated with the new ventures in a more prudent way.

The policies are introduced to make aware the business units prior to engaging in new activities and to prevent any losses or impact faced by the bank while engaging in businesses and to protect against any windfalls. Therefore, the policy will carry out a balancing act between optimum gains and the minimum losses of businesses and as a guideline for future risk management controls required by the business units.

In carrying out the function's followings are the main type of Risks that would be faced by the banks.

- Credit Risk
- Market Risk
- Liquidity Risk
- Operational risk
- Information / Cyber Security Risk
- Legal Risk
- Compliance & Reputation Risk

This document will discuss in brief how the controls are imposed to mitigate same and duties and responsibilities of each unit with monitoring authority of same. This policy is in compliance with the requirement set in the Banking Act Direction No 07 of 2011 and Section 9 of the CSE listing rules on Corporate Governance (Issued in Sep 2023).

1.2. Objectives of the Risk Management Policy

The main objective is to have a directive on controlling, monitoring, and reporting of the risks that may affect the functions of the bank. The risk is considered important by the management of the bank and taking appropriate action and preventing an impact on the financial position is another factor which would focus under this policy.

The objectives of the policy will be achieved by

- Inculcating a risk management culture within the bank with the initiative from the top of a framework of integrated risk management guidelines.
- To introduce best practices in the industry and benchmark the bank's risk policies.
- To record and monitor threats faced by the bank and to evaluate opportunities available in a methodical manner.
- To define the risk exposure and identify the same at required levels.
- To assist calculated risk taking and ensure conscious decisions are taken with proper evaluation.
- To strengthen the risk-based pricing system in place.

02. DETAIL POLICY

2.1 Role of the Board of directors

The planning responsibility of risk identification and understanding made by the Board of directors will be the framework for management of risks in the bank. The required activities and the techniques will be broadly done by way of following which will address all dimensions which impact the risks.

- Management and monitoring of activities through Board Sub Committee; Integrated Risk Management committee.
- Adopting of written systems, policies and procedures which relate to management of Risks.
- Ascertaining and identifying tolerance levels/Limits of risks.
- Defining quantitative and qualitative risk goals.
- The relative behavior of risk exposures and connected outstanding in relation to capital of the bank.
- Ensure compliance with the policies incorporated and the regulator requirement through a sound mechanism to monitor risk exposure.
- Introducing and directing robust systems for internal controls from time to time

2.2 Responsibilities and Users

The requirement of this policy should be applied primarily by the Board Integrated Risk Management Committee and all staff of the Bank including those employed on a contract basis. Any deviations by staff will be subject to disciplinary action. Therefore, submission of accurate information on a timely basis as required by members of the Committee is considered imperative for effective implementation of this policy.

03. BOARD INTEGRATED RISK MANAGEMENT COMMITTEE (BIRMC)

3.1. The composition and responsibilities

The main duty of the BIRMC would be to identify, monitor, measure and make recommendations on the overall risk profile of the bank in an integrated manner. The committee will function on the charter and will review the risk management policy and guiding principles on all aspects of risks in the bank. It will also review the standing of the bank in relation to regulator's requirements and adherence to same by the bank. The committee will also propose systems and procedures to be adopted on any future risk monitoring areas of development as a way forward in developing the risk mitigating factors to the next level.

The committee will review the ALCO minutes and the Stress testing scenarios in addition to the risk-goal monitoring. The volatility in portfolio values identified will be one of the main topics discussed and the action required will be discussed whenever necessary.

3.2 The Structure of the Committee

BIRMC shall consist of a minimum of three (03) Non-Executive Directors out of which a minimum of two (02) or the majority of the members shall be Independent Directors.

Director / Chief Executive Officer, Chief Risk Officer and management personnel supervising broad risk categories namely Credit, Market, Operational, Information security risks and Compliance will be permanent invitees.

Accordingly, Board Integrated Risk Management Committee (BIRMC) of Pan Asia Banking Corporation PLC will consist of following members:

Three (03) Non-Executive Directors out of which minimum two (02) or majority of the members shall be Independent Directors.

Permanent Invitees of the Committee,

i. Director/ Chief Executive Officer
ii. Chief Risk Officer
iii. Manager II - Integrated Risk as the Secretary to the Committee.
iv. Chief Compliance Officer
v. Officer in Charge of Credit Risk
vi. Officer in Charge of Treasury Middle Office
vii. Officer in Charge of Information Security (with in the Risk Management Unit)
viii. Information Security Officer (ISO)

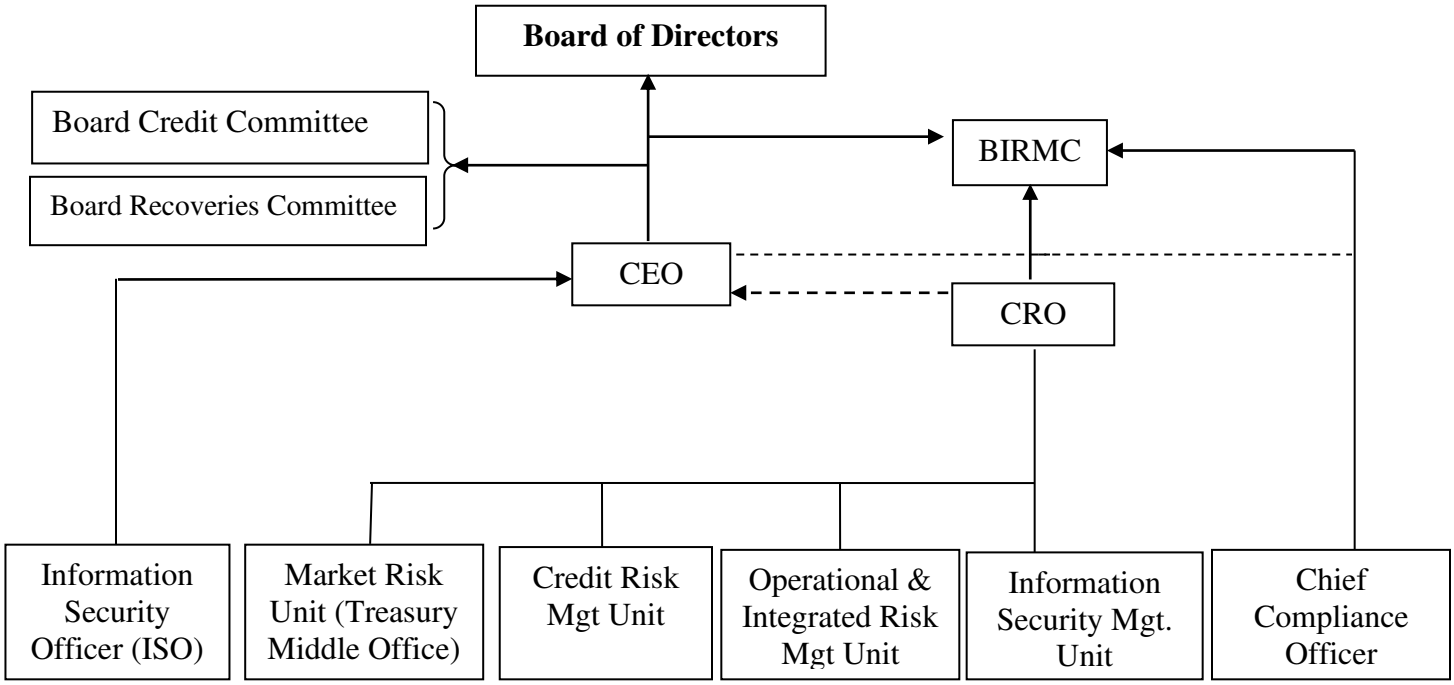
Also, the officer can nominate the staff member who acts in his/her absence to attend the meeting. Manager II - Integrated Risk will act as the Secretary to the Committee. (Depending on the need to fulfill this requirement from the available members of the Committee, any other member can be appointed as the Secretary.) The Chief Risk Officer will act independently of the business units and monitoring of Credit, Market, Operational and Information security related risks will be under his purview. The Bank has appointed a Chief Compliance Officer (CCO), who will be the in charge for the compliance function of the bank and CCO directly reports to BIRMC. The Committee may invite any key management personnel for participation at the meetings depending on the subject matters under discussion in the agenda.

3.3 Operational Procedures, Guidelines and Risk Goal Monitoring.

The operational procedures and guidelines are established under the directive of the Board. These guidelines will in turn have to be followed at operational levels where risks are actually created by the staff who take risks on behalf of the bank in the process of providing banking services to customers or providing support services to the business units, viz front office, credit relationship, dealers, support services staff etc. The principles to follow in adopting such guidelines, policies and procedures are broadly set out below. The risk goals to be monitored by BIRMC are indicated elsewhere in this document.

- **Organization Structure**

A sound organization structure is a pre-requisite for successful implementation of Risk Management system. The following elaborates Pan Asia's existing Risk Management function.



3.4 Credit Risk

Credit Risk is identified as the possibility of losses or impact arising due to diminution in the credit quality of borrowers or counter parties in relation to lending, trading, hedging, settlement, and any other financial transactions. These losses could arise from default by individual, corporate, other counter parties both locally and internationally due to their inability or unwillingness to meet the commitment. Credit Risk could arise from the banking book and the trading book/or both on or off balance sheet.

3.4.1 Components of Good Credit Risk Management Systems

- Credit policies, strategy, and process.

Bank is required to adopt policies and procedures in monitoring credit in the organization. Policies are the foundation on which Credit Risk Management of both portfolio and processes are built. The main policies/tools, which are currently used for credit management are;

- Credit Policy Manual
- Credit Risk Management Policy
- Product Related Policies – (Leasing , pawning , Consumer Credit ext)
- Write off / write-down Policy.
- Social and Environmental Management System (SEMS) Policy
- Policy on internal Borrower Risk Rating & Risk Based pricing.
- Policy on Loan Review Mechanism (LRM)

- Policy on CRIB reporting
- Stress Testing Policy
- Policy on Classification, recognition and measurement of Credit exposure
- Policy on adoption of SLFRS 9 Financial instrument
- Policy on Valuation of Immovable Properties
- Delegated authority limits

New policies adopted will be vetted by the Board Credit Committee and submitted to the Board for approval.

Credit strategy will be adopted according to the established objectives and goals of the bank's credit granting activities and will be according to the organization's credit appetite and the acceptable level of risk-reward tradeoff for it's activities and will be initiated by Head of Risk.

- Credit Process

  Credit process is laid down in the Manual on Credit Policy and Procedure. Same is also in accordance with the internal control system of the bank. Other than facilities backed by Cash and Sammana products, all other disbursements of facilities are done through an independent authority, the Credit Administration Unit.

  Board Credit Committee besides its functions in an advisory capacity is the approving authority for large credit proposals. The functions of the committee are described in the charter document.

- People and Credit Culture

  Selection of staff and their development of expertise is especially required to establish and sustain a good credit culture. The bank will adopt best practices in the industry to ensure good credit culture & asset growth.

3.4.2. Credit Risk Goals

The main purpose of having a risk adjusted model is to ensure optimum allocation of capital and derive adequate return on the allocated capital. Weighted against the expected rewards in terms of Return on Risk Weighted Assets (RORWA) and Risk Adjusted Return on Capital (RAROC) the following goals are identified by the BIRMC for monitoring under Credit Risk.

i. Stage 3 Impaired loan from Total Lending Book
ii. Stage 3 Loans, net of stage 3 Impairment Provision of the bank to the total loans
iii. Bank should endeavor to maintain the open credit exposure ratio.

iv. Stage 3 Impairment against Stage 3 Loans.
v. Composition of loan book of different risk grades,
vi. Movement of the non-performing assets in absolute terms during the period compared to the previous quarter.
vii. Exposure to a single borrower should not exceed the limits prescribed by the Central Bank of Sri Lanka.
viii. Sectorial exposure of the loan book should not exceed the approved exposure limits set by BIRMC:
ix. Breaches reported under lending product exposure limits set by BIRMC
x. Breaches reported under limits on segmentation of Bank's lending Book set by BIRMC
xi. Breaches reported under Related party lending exposure limit set by BIRMC
xii. Overall Stress testing results should be maintained at the level approved by the BIRMC

3.5 Market Risk, Liquidity Risk, and Interest Rate Risks

3.5.1. Market Risk Monitoring Policies

The potential impact on movements of the market prices adversely in relation to the value of a tradable instrument is broadly identified as Market Risk. Since bank deal mostly in price sensitive assets and liabilities the evaluation of potential impact of the market activities will assist to identify risks that will impact on the trading activities. Any impact due to illiquidity of the instruments and the interest rate volatility which may incur due to such positions should be evaluated and prudent steps should be taken to minimize losses. Relevant tests should be done to incorporate extreme events and shocks should be captured on portfolio vulnerabilities based on market developments.
The bank will discuss the action and remedies for such changes based on its “Treasury Procedure Manual” which should be approved by the Board as required by the bank from time to time.

3.5.2. Market Risk Goals

Considering the level of importance of Market Risk Management, the following goals are determined currently for monitoring at the BIRMC.

i. Statutory liquid asset ratio should be maintained within the limit prescribed by Central Bank.
ii. Statutory Reserve Ratio(SRR) should be maintained not less than the percentage prescribed by the Central Bank of Sri Lanka
iii. Liquidity Covering Ratio should be more than the regulatory requirement.
iv. Interest Rate Risk should be within the banks internal limit
v. Securities held in the Trading portfolio should be within the internal loss limits

vi. Net open position to be maintained within the limits prescribed by the Central Bank of Sri Lanka
vii. Cross currency trading-take profit and losses should be within the internal take profit and loss limits
viii. Brokerage paid to each broker to be within the banks internal limits
ix. Measurement of Value at Risk to be within the internal bank limit
x. Results of stress testing in relation to Liquidity and forex activities should be within the banks' internal limits.
xi. Key Borrowing clients and key deposit clients exposure to be within the internal bank limit

3.6. Operational Risks

3.6.1. Operational Risk Management Framework

Operational Risk is intrinsic to every financial institution, and it should be an important content of our bank wide risk management framework. Banks with a strong culture of risk management are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that occur. The framework outlines the internal operating policies of PABC's Operational Risk Management Framework and sets out a context that complies with regulatory requirements as well as internal requirements towards managing Operational Risks.

Operational risk is relevant to every aspect of the bank's business and covers a wide spectrum of issues. Losses arising through fraud, unauthorized activities, errors, omission, inefficiency, system failure or from external events all fall within the operational risk definition.

Operational Risk is defined as: The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

The management of Operational Risk comprises:

- Identification
- Assessment
- Monitoring & Control of Operational Risks
- Reporting

Given below are the relevant policies and procedures relevant to Operational Risk Management of the bank.

- Operational Risk Management Policy
- Operational Risk Incident Reporting & Loss Write Off Procedure

- Procedure on reporting of operational risk related incidents to Operational Risk Management Unit (Incident Reporting Management System - EFAC System)

3.6.2. Operational Risk Goals

Arising out of the risk indicators and guidelines, the following goals are identified under operational risks to be achieved by the banks.

i. Operational losses not covered by Insurance over net income for the reporting period
ii. Results of Branch/Departments/IS audits carried out
iii. Number of complaints received for not receiving account/ credit card statements over total statements dispatched.
iv. Report on detection of internal frauds/attempts.
v. Report on detection of external frauds/attempts.
vi. To maintain staff turnover ratio on acceptable level
vii. No of unplanned core banking system down times
viii. No of unplanned ATM down times
ix. Delays in submitting clearing cheques.
x. Unreconciled / unidentified outstanding in suspense accounts
xi. Number of cheques returned due to lack of funds over out of total cheques presented.
xii. Availability of succession plan at strategically important/ specialized departments
xiii. Total number of complaints received during the period over total number of calls answered.

3.7 Information Security

"Security" in relation to information shall mean the maintaining of Confidentiality, Integrity and Availability, properties of the information, as per the following definitions:

- **Confidentiality** - Information should not be made available or be disclosed to unauthorized entities (i.e. persons, organizations, and systems);
- **Integrity** - Reliability of information will be maintained through protection from unauthorized, unintended modifications during transmission, storage, and retrieval; and
- **Availability** - Authorized users are granted timely and uninterrupted access to information. Availability will be based on the business requirement of the user.

Bank shall strive to secure information, safeguard information/ IT assets and develop efficient information systems by:

i. Being committed to protecting bank's critical information from intentional or unintentional unauthorized disclosure, modification, or destruction throughout its lifecycle. This protection includes an appropriate level of security over the assets used to process, store and transmit that information while aligning with the Bank's strategic goals.

ii. Maintaining an effective information security posture at Pan Asia Banking PLC (PABC). Following information security objectives are expected to be achieved:

- Implement, enforce, and conduct periodic review of information security policies, procedures, guidelines, and checklists.
- Establish safeguards to protect PABC's information/information systems from theft, abuse, Leakages, misuse and any form of damage(s) / Potential damage(s);
- Understand the specific challenges associated with system access, and designing, deploying and maintaining successful access controls.
- Conducted privilege / user access reviews for all critical systems quarterly to ensure the access controls and information security of the Bank.
- Encourage management and staff to maintain an appropriate level of awareness, knowledge, and skill to allow them to minimize the occurrence and severity of information security incidents and breaches.
- Information security weaknesses and incidents are identified, recorded and responded to in a timely manner.
- Ensure physical & logical access controls in place to enhance information security.

i. Ensure of PABC's technology infrastructure "Change Management Process" - *When Bank begins to use a change information resource (software, hardware, networks, system documentation, and environment) for any reason including but not limited due to system or infrastructure enhancement, it should be managed according to a specific process called a "change management processes", fixed in advance so that the transition is accomplished in an organized way in all its steps from the review to the authorization, test, implementation, and release of the changed resource;*

ii. Ensure the proper preventive and detective measures are taken against potential threats through "Patch Management". - *Patches apply to many different parts of the banking information system which include operating systems, servers, routers, desktops, email clients, mobile devices, firewalls, and many other components that exist within the network infrastructure;*

- Ensure availability of information systems by providing recommendations for minimum downtime.
- Ensure the utilization of storage capacity and adequate level of monitoring is being carried out to avoid unnecessary interruption.

- Ensure appropriate application, operating system, database, and network security controls are implemented and weaknesses are identified.
- Ensure all critical information for the bank is backed up and restoration testing has been conducted.
- Implement information security controls for 3rd party services, which may safeguard bank sensitive information; and
- Working with third-party cyber security specialists to enhance cyber security among PABC culture.
- Ensure all data are being classified based on information security sensitivity level and labeled with assigned classification by enforcing required policies.
- Ensure all E-mails are classified based on the information security sensitivity level and labeled with assigned classification by enforcing required policies.
- Ensure industry standard SIEM tool is in place which capable of log consolidation, event correlation and incident management.
- 24x7 Security information and event management (SIEM) Monitoring mechanism/ Security Operations Centre to be established for online threat monitoring and prevention through incident response.
- Implement Mobile Devices Management requirements for Bank provide Mobile phones to ensure information security in the Bank.
- Privilege Access Management system (PAM) is available to maintain administrative access management.
- Software Licensing to be purchased, and update appropriately.
- System patching, Vulnerability Assessment and Penetrating Testing (VAPT), and remediation to be attended to appropriately.
- Awareness of the Industry level information security threats and necessary actions shall be taken.

iii. Evaluate the appropriateness of technology infrastructure in order to address business requirements effectively and enhance the efficiency of business operations.

iv. Proactively assess risks that may harm PABC's information systems.

v. Maintaining the compliance with any applicable legal, regulatory, contractual obligations and based on the latest industry security standards (for example: ISO/IEC 27001:2013, Payment Card Industry Data Security Standards and Central Bank guidelines, etc.) while preserving PABC reputation and image.

vi. Identify and report any violations of the information security policies.

The Information security related matters are being handled by Bank's Information Security Officer (ISO) and the Officer attached to the Risk Management unit as per the assigned duties/responsibilities in line with the CBSL direction No 16 of 2021 on "Regulatory framework on technology risk management and resilience for licensed Banks".

Risks arising from compliance, reputational management, legal, stability and IT etc. are also considered important to be controlled for functions of financial service sector. The risks which affect the reputation should be identified and prioritized for establishing strategies to protect the reputation of the organization if we are to avoid a crisis of confidence among the stakeholder, especially the wider public i.e. customers/depositors.

3.8. Compliance, Reputational, Legal and other Contingencies

3.8.1. Contingencies Risk management

3.8.2. Risk Goals to be monitored.

The following risk indicators and goals are to be monitored for the protection of relationships under the said contingencies.

<u>On Strategic</u>

i. Net Interest Margin should be maintained above the budget.
ii. Annualized ROA (before Tax) should be maintained the budget.
iii. Annualized ROE should be maintained above the budget.
iv. Capital adequacy ratio – TIER I should be maintained above the CBSL requirement.
v. Capital adequacy ratio – TIER II should be maintained above the CBSL requirement.
vi. Cost/Income Ratio should be maintained below the budget.
vii. CASA / Total deposit Ratio should be maintained above the budget.
viii. The YTD Deposit growth rate should be maintained above the budget.
ix. YTD lending growth rate should be maintained above the budget.
x. Maintaining Fitch Credit Rating.

<u>On Compliance</u>

xi. Breaches reported under Submission of Regulatory / statutory returns.
xii. Number of cautionary letters received from regulators &imposed fines.
xiii. No of reported regulatory breaches (KYC/AML ect)
xiv. Number of Suspicious Transactions Reported (STR) submitted to FIU.
xv. Maintaining of CRIB reporting data acceptance ratio

<u>On Legal</u>

xvi. Legal cases against the Bank which have material impact In values.

Information Security

xvii. All Baseline security standards should be achieved more than the target given by BIRMC.

Strategic Risk Management

The Bank's Board BIRMC pursues the risk indicators / goals and will make recommendation for Strategic Risk Management.
The key areas for such recommendation would be;

- Improvements to segmentation mix of business.
- Threats identified in industries.
- Liquidity management arising out of ALCO.
- Monitoring of compliance breaches and controls to be imposed.
- Changes due to direction of the regulator.
- Recommendation from the Internal Audit based on the lapses identified in the Business Units.

3.9 Reporting Procedure

The respective Business and supporting units are required to report on the positions of risk goals to the Risk Department on monthly basis. The Risk Department will compile the reports and submit to the BIRMC with necessary review and recommendation for detailed delibration.

Based on the said observations and recommendations, a report will be submitted to the Board on risks goals monitored by the bank highlighting the areas of concern. If any further recommendations are made by the Board such will be notified to the relevant units for adherence. Progress of which will be reported to the next board meeting or the next BIRMC. Continuous improvement and more prudent methods of monitoring will be one of the main objectives of the bank wide risk management procedure for mitigating new threats faced by the bank. Risk Goals and the tolerance limits are reviewed periodically by BIRMC in line with the bank's overall strategic objectives and risk appetite.

3.10 Prevention and Remedies available

Bank will be required to maintain adequate insurance coverage over all properties and other insurable risks of the Bank. The Administration Department will be maintaining Insurance Register (except for following) and will be responsible for coordinating with insurance companies and for annual renewal of policies.

- Human Resources will handle insurance of staff connected policies
- Bank's indemnity of operational functions by operations department.

3.11 Conclusion

This policy will cover the main factors which will affect the functions of the bank. The monitoring will commence with the risk goals mentioned therein and at the initial levels. Interim reviews will be introduced if necessary for amendments required for urgent changes in the policy from time to time.

However, this policy will be reviewed by BIRMC at least annually. New goals, if any, will be added when required.

The requirements of the regulator, industry best practices and the identified Key Risk indicators of the bank are considered when preparing this policy document.