RISK MANAGEMENT POLICY

Document No : PLC – RMP - 001

Classification : Internal

Owner : Risk & Control Department

Effective Date : 06.06.2017

Document History:

Release Date	Revision No	Author(s)	Description	Recommended By	Approved By
06.05.2017	1.0	Chief Risk Officer	Initial release	BIRMC	Board of Directors
30.07.2020	1.1	Chief Risk Officer	Amendment	BIRMC	Board of Directors
26.05.2023	1.2	Chief Risk Officer	Amendment	BIRMC	Board of Directors

1. PURPOSE

The purpose of this Policy document is to define People's Leasing & Finance PLC's ("PLC" or "the Company") overall risk management policies and framework and act as point of reference to all staff of the Company.

2. DEFINITION OF RISK

Risk is the possibility that the outcome of an action or event could bring up adverse impacts. Such outcomes could either result in a direct loss of earnings/capital or may result in imposition of constraints on the Company's ability to meet its business objectives. Such constraints pose a risk as these could hinder the Company's ability to conduct its on-going business or to take benefit of opportunities to enhance its business.

3. BACKGROUND

As the largest non-bank financial institution in Sri Lanka, providing a full spectrum of financial services to a wide clientele of clients scattered around the island, PLC is exposed to the full gamut of risks ranging from credit and market to reputational and operational. The Company is fully cognizant of the need for sound risk management practices to ensure its growth, stability and long term viability.

Risk Management is a discipline at the core of the Company and includes all the activities that affect the Company's risk profile. It involves identification, measurement, monitoring and controlling risks to ensure that:

a) The individuals who take or manage risks clearly understand it.

b) The Company's risk exposure is within the limits established by the Board of Directors.

c) Risk taking decisions are in line with the business strategy and objectives set by the Board of Directors.

d) The expected pay-offs compensate for the risks taken.

e) Risk taking decisions are explicit and clear.

f) The Company is in compliance with all applicable laws and regulations of the country and with the governance standards prescribed.

g) Application of high and consistent ethical standards to the Company's relationships with all customers, employees, and other stakeholders.

h) Activities are undertaken in accordance with fundamental control standards. These controls will employ the disciplines of planning, monitoring, segregation, authorisation and approval, recording, safeguarding, reconciliation, and valuation.

i) Sufficient capital as a buffer is available to take risk.

4. STRATEGIC VISION

The Company's strategic vision with regard to risk management includes the proactive and integrated management of the risks that the Company encounters in its business activities whilst maximizing capital efficiency.

Risks will not be viewed and assessed in isolation, not only because a single transaction might have a number of risks but also because one type of risk can trigger other risks.

Since interaction of various risks could result in diminution or increase in risk, the risk management process should recognize and reflect risk interactions in all business activities as appropriate.

Whilst assessing and managing risk, the Management should have an overall view of risks the Company is exposed to. This requires having a structure in place to look at risk inter-relationships across the organization.

5. OVERALL POLICY STATEMENTS

5.1. It is PLC's policy to manage its portfolio of risks in an integrated and systematic manner through a combination of structure, systems and processes.

5.2. It is PLC's policy to maintain a well-diversified portfolio of credit and other risks which produces reliable and consistent risk adjusted returns while operating within the Company's overall risk appetite and tolerance limits.

5.3. It is PLC's policy to pay due care and attention to individual and aggregated risks as long as the Company is exposed to such risks.

6. RISK MANAGEMENT FRAMEWORK

6.1. Three-Lines of Defence Model

The Three-Lines of Defence Model facilitate the accountability and transparency through clear identification and segregation of roles with respect to risk management and governance activities. The Company's Risk Governance Model can be depicted as follows.

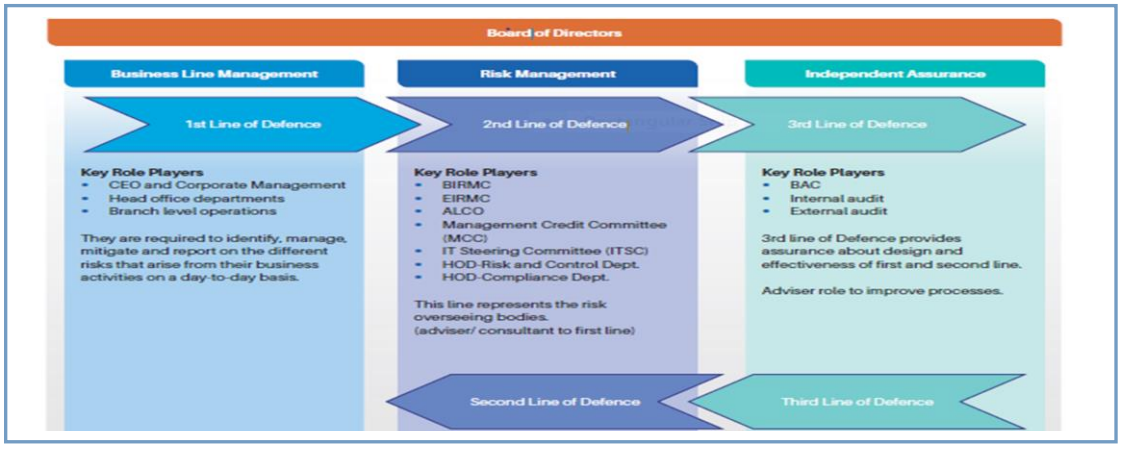

Figure 1

6.2. The Board of Directors and its responsibilities

The Board of Directors of PLC is ultimately responsible for the management of risks and the Company's overall risk appetite. With the delegated authority of the Board, the Board Integrated Risk Management Committee (BIRMC) shall assess the impacts of risks, including credit, market, liquidity, operational, strategic, compliance and technology through appropriate risk indicators and management information and make recommendations on the risk strategies and the risk appetite to the Board.

6.3. First Line of Defence

The Company recognises the Business Units as owners of the risk and the first line of defence. They are required to identify, manage, mitigate and report on the different risks that arise from their business activities on a day-to-day basis.

6.4. Second Line of Defence

The second line of defence includes the risk management and oversight function, which mainly comprises the BIRMC, ALCO, Management Credit Committee (MCC), IT Steering Committee (ITSC) and EIRMC. These Committees design and deploy the overall Risk Management framework, develop Risk Management methodologies, policies and procedures, approve and review various risk exposures within the parameters laid down by the Board and undertake aggregated risk reporting. The policies and procedures are reviewed on a regular basis and updated in line with the changes in market conditions, products and services offered.

Head of Risk reports to the BIRMC every two months and represents in ALCO, ITSC and MCC meetings. The Compliance officer reports to the BIRMC on the status of Company's compliance with regulations, policies and procedures every two months.

6.5. Third Line of Defence

The third and last line of defence is Internal Audit which provides independent testing and verification of the effectiveness of the risk management framework, including policies and procedures and compliance with these policies and also assesses management assurance processes. The Internal Audit should report directly to the Board Audit Committee (BAC) so as to ensure its independence. External audit also forms part of providing independent assurance.

7. EXCEPTIONS

To ensure that risk taking remains within limits set by the Board of Directors, any material exception to the risk management policies and limits should be reported to Board of Directors/Senior Management that in turn will trigger appropriate corrective measures. These exceptions also serve as an input to judge the appropriateness of systems and procedures relating to risk management.

8. LINKAGES

This policy document is not a standalone document and must be read in conjunction with the Company's other operating circulars and CBSL directions in general and in particular the following:

- Risk Appetite and Tolerance Statement
- Credit Policy
- Margin Trading Credit Policy
- AML and KYC Policies
- Product Procedure Manuals
- Write-off Policy
- Policy on Valuation and Inspection of Immovable Properties
- Impairment Policy and Guidelines
- Post Disbursement Review Policy
- Early Warning Monitoring Mechanism to the Company Recovery Process
- Recovery Manual
- Gold Loan Manual
- Compliance Policy Manual
- Policy on Outsourcing of Business Operations
- CCTV Operating Policy
- Consumer Complaint and Grievance Handling Policy
- Pricing Policy
- PLC Whistle Blower Policy
- Stop Loss Policy on Share Transactions
- All ICT Policies including Policies on Information Security, Disaster Recovery, Cyber Security, ect.
- Treasury Policies: Treasury Procedure Manual, and Liquid Assets Investment Policy and Procedure
- Code of Best Practice in Corporate Governance
- Stress Testing Policy
- HR Policy
- Business Continuity Plan
- Board level Committee TORs (Board Credit Committee, Board Integrated Risk Management Committee, Board Audit Committee)
- Management level Committee TORs (Management Credit Committee, Executive Integrated Risk Management Committee, ALCO)
- ICAAP Document

9. ROLES AND RESPONSIBILITIES

The Risk Management framework will encompass the full scope of risks to be managed, the processes, systems and procedures to manage risk and the roles and responsibilities of committees and individuals involved in the risk management. The framework should be comprehensive enough to capture all risks the Company is exposed to and will have flexibility to accommodate any change.

The individuals responsible for review function (Risk review, Internal Audit, Compliance etc.) should be independent from risk taking units and report directly to the Board or Senior Management who are also not involved in risk taking.

9.1. Board of Directors

The Board of Directors of PLC will be responsible for setting the overall risk appetite and oversight of the risk management process and will act through the Board Integrated Risk Management Committee.

9.2. Risk Management & Control (RMC) Department

The RMC department needs to function completely independent from the business functions. The organisation structure of the Risk Management function is set out below:

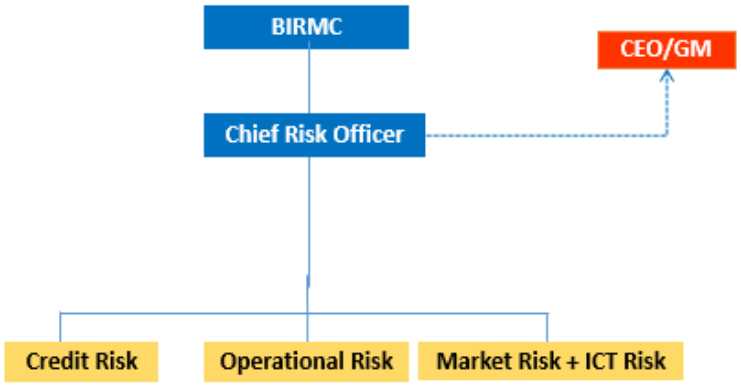

Figure 2

9.2.1. Roles and Responsibilities:

The risk management department would be responsible for:

a) Preparing the Risk Policies & Frameworks and carrying out periodic reviews.

b) Assessing the corporate risk profile of the Company which consists of Credit Risk, Market Risk, Liquidity Risk, Operational Risk, Regulatory Risk and Strategic Risk on a monthly basis and report the same through Risk Dash-board reports to the BIRMC once in every two month.

c) Assisting the Board in its development of the Company's risk appetite and translating the risk appetite into a risk tolerance limits structure.

d) Carrying out periodic reviews on the risk tolerance limits to reflect the changes in the business environment, regulatory framework.

e) Making representations in the strategic planning process of the Company.

f) Overseeing the risk-taking activities across the business operations and the development and implementation of the Company's risk management function including Business Continuity Policies.

g) Coordinating with the Internal Audit to ascertain the effectiveness and implementation of the existing controls.

h) Coordinating the BCP implementation process liaising with the external BCP consultant and the operational departments ensuring effective and up-to-date Contingency Planning and Disaster recovery planning measures are in place across the Company.

i) Conducting stress tests on a quarterly basis and assess the impact on the Company on account of Credit, Market and Liquidity risk exposures undertaken by the Company.

j) Ensuring that risks that have a High Impact and/or High Frequency are adequately transferred by means of appropriate insurance arrangements.

k) Assessing the risk profile of subsidiary companies and forwarding Risk Dash-board reports/Risk indicator reports to the BIRMC for the review.

l) Submitting a Risk Dash-board report which contains the assessment of risk profile of PLC to the Parent Company on a quarterly basis.

m) ICAAP process of the Company and for maintenance and periodic update of ICAAP.

9.3. Business/ Unit Heads

Business and Unit Heads, along with their teams are responsible for the Identification and management of all risks within their functional responsibilities.

9.4. Internal Audit Department

Internal Audit is responsible for independent review of the control environment, and for monitoring, reviewing and reporting on compliance with policies and procedures.

It also provides the Board with assurance on the effectiveness of risk practices and procedures.

10. CREDIT RISK

Credit risk arises because the Company's customers and counterparties may fail to meet their contractual obligations and derives principally from the loans and advances made to and due from them and counterparties.

10.1. Organisation Structure for Managing Credit Risk

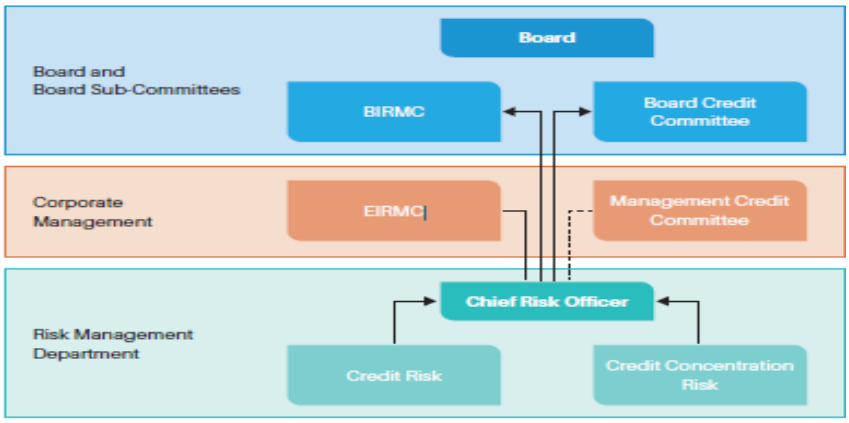

Figure 3

10.1.1. The Board will delegate the responsibility of the oversight and management of credit risk to the Management Credit Committee, Risk & Control Department and Credit Department, which includes:

a) Formulating and updating credit policies in consultation with the Risk Management & Control department and Business Units.

b) Establishing credit approval structures so as to ensure that the larger and higher risk exposures are reviewed and approved at the appropriate levels of seniority.

c) Periodic review of individual credit exposures and overall portfolio to ensure that there are no undue risk concentrations.

d) Adequacy of provisions and management of higher risk exposures.

e) Developing and maintaining risk rating systems for the products with high risk element such as loans, as a means of quantification of credit risk, differentiating between the various levels of risk and determining the degree of control and supervision required.

10.1.2. Internal Audit should conduct regular audits of the Branches and Business Units to provide assurance of the adequacy of controls and an independent assessment of the risks to Senior Management and the Board Audit Committee.

10.1.3. Risk Management & Control department assesses the credit risk and the credit concentration risk at the portfolio level based on key Credit Risk Indicators set out in the risk tolerance statement and regular credit risks reviews and analysis and report every two months to the BIRMC for the review.

10.1.4. Specific Credit Policies are contained in the Company's Credit Policy Manual. This should be read in conjunction with all relevant Central Bank of Sri Lanka circulars and guidelines.

11. MARKET RISK

Market risk is the risk that changes in foreign exchange rates, interest rates and equity prices will adversely affect the Company's income and or the value of any financial instruments that it may hold.

11.1. Organisation Structure for Managing Market Risk Section

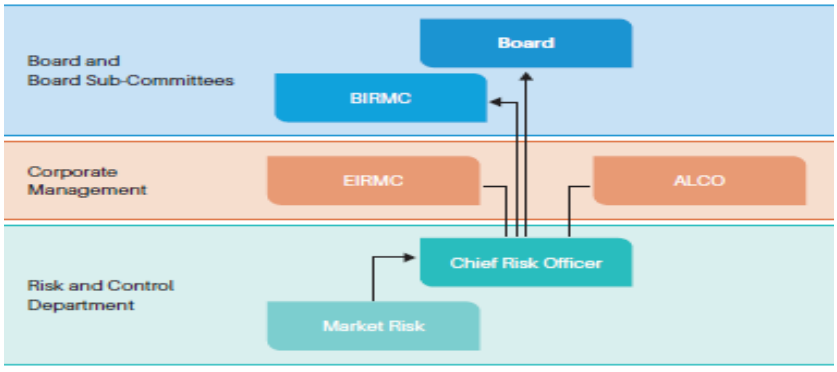

Figure 4

11.1.1. For the management of market risks, the Board will, on the recommendations of the ALCO, set limits for the various Treasury related activities.

11.1.2. The ALCO is responsible for the development of market risk management policies whilst the Treasury is responsible for the day-to-day monitoring of exposures against these policies. The Treasury however is primarily responsible for the overall management of market risks on an on-going basis.

11.2. Interest Rate risk

11.2.1. Interest Rate risk is the possibility that changes in level of market interest rates will adversely affect the Company's net interest income and the value of any financial instruments held.

11.2.2. The ALCO is responsible for managing interest rate risk by setting and monitoring limits for interest gaps and matching the repricing profile of the various interest sensitive assets and liabilities.

11.2.3. Risk Management and Control department assesses the interest rate risk based on interest rate risk indicators against set risk tolerance limits.

11.2.4. Risk Management and Control department performs stress tests on interest rate risk on a quarterly basis.

11.3. Foreign Exchange risk

11.3.1. It is the Company's policy to keep no foreign currency in open position and such exposures thereby should be hedged immediately against the risk.

11.4. Equity Investment Risk

11.4.1. The equity investment portfolio should be maintained below the volume limit set by the Board.

11.4.2. ALCO is responsible for reviewing the position report which includes net capital gains or losses on a regular basis.

11.5. Commodity Risk

11.5.1. Risk and Control Department regularly monitors the gold price volatility and performs stress testing regularly or immediately if the operational environmental changes are significant.

12. LIQUIDITY RISK

Liquidity risk is that the Company will not be able to meet its contractual obligations as and when they arise. It also encompasses the difficulty to fund assets at appropriate maturities

and rates, and the inability to liquidate assets at a reasonable price in an appropriate time frame.

12.1. Organisation Structure for Managing Liquidity Risk

The same orgainisation structure for market risk depicted in 11.1 above will apply for the liquidity risk management.

12.1.1. The Company's Treasury is charged with the responsibility of managing the Company's liquidity within both internal and regulatory guidelines, under the supervision of the ALCO.

12.1.2. In addition to the above, liquidity risk should be managed by:

a) Gap management of cash flow maturities (on residual, contractual and behavioural basis)

b) Maintaining a portfolio high quality liquid assets that can be easily converted to cash to meet any contingencies

c) Having ready access to the inter-bank money market

d) Stress testing of liquidity positions to assess the vulnerability of the Company to any unlikely but potential threats and extent of reliance on any particular source of funds.

e) Contingency planning

12.1.3. Risk Management and Control department assesses the Liquidity risk based on liquidity risk indicators against set risk tolerance limits.

12.1.4. Risk Management and Control department performs stress tests on liquidity risk regularly.

13. OPERATIONAL RISK

Operational Risk is inherent in all businesses and is the risk of direct or indirect impacts resulting from inadequate or failed internal processes or systems or from external events. Operational risk cannot be totally eliminated and the challenge is to manage and contain any operational losses within acceptable levels as determined by the Board.

13.1. Organisation Structure for Managing Operational Risk

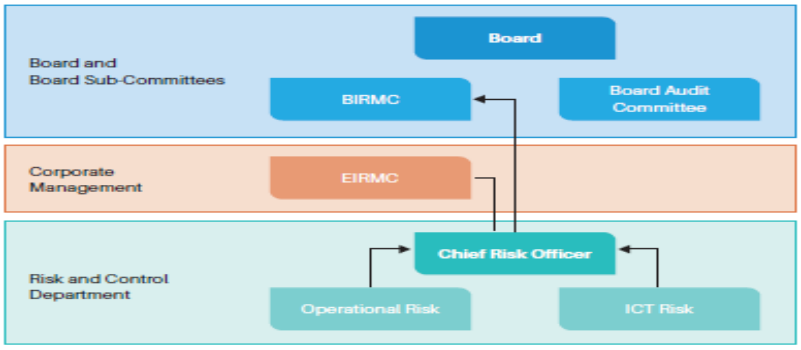

Figure 5

13.1.1. The Board of Directors is responsible for establishing strong Internal Control Framework in defining the roles and responsibilities of all staff, branches and business and functional units in the management of operational risk. This includes risk identification and assessment, capturing and reporting of risk events, appropriate segregation of duties, dual controls, business continuity planning and on-going review of controls and procedures.

13.1.2. The prime responsibility for the control of operational risk lies with the branches and business units where the risks originate.

13.1.3. Internal Audit should evaluate the adequacy of internal controls in assessing related risks and conduct regular operational reviews to identify any bottlenecks and loopholes in the process at business units and branches.

13.1.4. The RMC department is responsible for assessing the operational risk, methods such as Branch operational Risk Self-Assessments, Incident Reporting, audit findings and monitoring of the trends of operational key risk indicators etc. will be used for this purpose.

13.1.5. In managing operational risk, HR department is responsible for creating the awareness, including high standards of ethics and integrity among the employees of the Company in line with the HR Policy.

13.1.6. ICT department should ensure robust information system security structure and adequate data recovery plans are in place.

13.1.7. Internal Audit, ICT and HR departments are required to report to the Risk Management & Control department on the operational risk events and losses at least on a quarterly basis.

14. COMPLIANCE RISK

Compliance Risk is defined as the risk of legal or regulatory sanctions, material financial loss or loss to reputation the Company may suffer as a result of its failure to comply with laws, regulations, and rules relates self-regulatory organization standards applicable to its operational activities.

14.1. Organisation Structure for Managing Compliance Risk

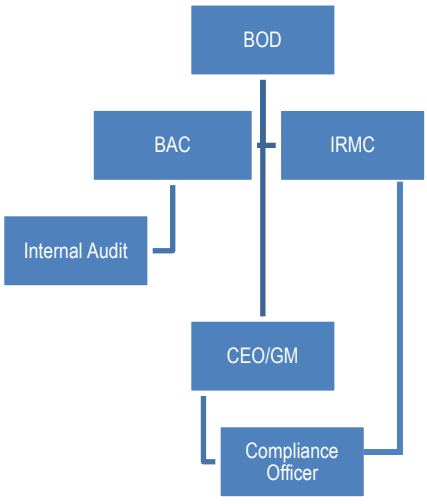

Figure 6

14.1.1. In order to avoid any violations of laws and regulations and to assure continued compliance with all relevant laws and regulations, the Board of Directors will ensure that a Compliance Program will be established and implemented under the guidance of the Compliance Officer.

14.1.2. A dedicated officer should be designated as the Compliance Officer to oversee the compliance status of the Company with the relevant rules, regulations and directions.

14.1.3. Internal Audit department shall carry out compliance audit annually and make audit reports available to the Corporate Management and the Board Audit Committee for their review.

14.1.4. Policy statements with regard to the management of compliance risk are;

a) It is the policy of the Company to always operate in a legal and ethical manner and to comply with all laws and regulations applicable to its business.

b) It is the policy of the Company that the Compliance Program is considered as a guideline to be followed by all members of the Board and staff.

- The Company requires that its Board members and staff, maintain high standards of integrity, and business ethics.
- The Board and employees must avoid any actions that are or appear to be inconsistent with such standards.

14.1.5. The Compliance Program is an on-going process designed to prevent and detect violations of the law, particularly money laundering and terrorist financing. If a situation should arise where there is a question about whether a proposed action is in compliance with a law, regulation or policy, all individuals should contact the Compliance Officer for clarification.

14.1.6. The primary responsibilities of the Compliance Officer shall include:

a) Develop and implement policies and procedures designed to eliminate or minimize the risk of breach of regulatory requriments;

b) Ensure compliance policies and procedures are clearly communicated to all levels of the Company to enhance the compliance culture;

c) Ensure reviews are undertaken at appropriate frequancies to assess compliance with regulatory rules and internal compliance standards;

d) Understand and apply new regulatory developments relevant to the structuring of new products and systems, to ensure conformity with the regulatory requirements, internal compliance and ethical standards;

e) Secure early involvement of design structuring of new products and systems to ensure with the regulatory requirements, internal compliance and ethical standards;

f) Highlight serious or persistent compliance issues and where appropriate, work with the management to ensure that they are rectified within the acceptable time;

g) Maintain regular contact and good working relationship with regulators based upon clear and timely communication and a mutual understanding of the regulator's objectives with highest integrity;

15. CAPITAL MANAGEMENT

PLC's primary objectives when managing capital are:

- to safeguard the Company's ability to continue as a going concern and to have sufficient capital to finance its expansion plans
- to optimize returns to its owners
- to comply with the regulatory capital requirements set by the Central Bank of Sri Lanka (CBSL)

The Company has developed the Internal Capital Adequacy Assessment Process for assessing overall capital adequacy in relation to its risk profile. ICAAP requires the Company to assign capital for additional risk not covered under pillar 1 of Basel II.

The Company shall maintain the capital in line with the minimum capital adequacy requirement as set out by the regulator and as guided by the ICAAP document.

a) The Company should consider how its capital requirement might change in line with its business plans over its strategic time horizon, and how it might respond to these changes.

b) Risk Management & Control department shall perform stress tests as a part of ICAAP under various scenarios.

16. MANAGEMENT OF OTHER TYPES OF RISKS

16.1. Strategic Risk

16.1.1. The Senior Management shall regularly review the effectiveness of strategy execution by referring comprehensive Management Information reports together with competitor analyses.

16.1.2. Strategy review will be carried out by the Risk Management & Control department and report the same to the CEO/GM, EIRMC, BIRMC and the Board on a quarterly basis.

16.2. Reputational Risk

16.2.1. Reputational risk is an event or incident that could adversely impact on the corporate brand and the Senior Management is responsible for following in managing the risk.

- Understanding the risk interdependencies
- Ensuring effective customer grievance handling procedures are in place
- Adherence to the corporate governance procedures by all employees

16.3. Socio-Economic & Political Risk

16.3.1. Socio-economic and political factors have a direct impact on the operational and investment activities of the Company and PEST analysis will be performed by the Risk Management & Control department in identifying any emerging risks.

16.4. Group Risk

16.4.1. Group risk relates to the loss (financial or non-financial) incurred by PLC through its subsidiaries and associates.

16.4.2. The Board of Directors of the parent company (PLC) is responsible for reviewing the performance of subsidiaries and associates including inter-company transactions.

16.4.3. The BIRMC is responsible for assessing the risk profile of each subsidiary operated with unique business models and recommending any risk mitigation action to the Board.

16.5. Risk of Unforeseen Events

16.5.1. This refers to the risk of business operations being disrupted due to unexpected events. Since this risk cannot be predicted with certainty in advance, the Risk Management & Control department should regularly assess the adequacy of insurance coverage and the validity of Business Continuity Plans.

16.6. Legal Risk

16.6.1. The Company's legal risks relate to inadequate or inefficient documentation, legal capacity, enforceability and the applicability of national law and dispute resolution mechanism in the jurisdictions under which it operates.

16.6.2. These risks are mitigated through procedures, precedence standard documentation and the legal review of all contractual documents of the Company.

16.6.3. The Company will use standard documentation developed over the years. The Legal department of the Company is responsible for the Company's contractual documentation i.e. to verify the legal capacity of the Company's counterparties, ensure the enforceability of the collaterals and to advise on the choice of governing law and forms of dispute resolution, before any contracts are entered into by the Company.

16.6.4. For this purpose, they may also, with the approval of the CEO/General Manager use the services of a competent outside counsel.

17. POLICY REVIEWS

This document and related policy documents should be reviewed and revised regularly to reflect changes in business environment, products and services offered.

18. APPROVAL

This policy document initially was approved by the Board of Directors BP No.72/2017 on 6th June, 2017.