ENTERPRISE RISK MANAGEMENT FRAMEWORK (ERM)

The Bank's philosophy is that responsibility for risk management resides at all levels within the Bank and therefore uses the three lines of defense model:

- The *first line of defense* rests with business units that are responsible for risk management. Assessment, evaluation and measurement of risk are ongoing processes and are integrated in the day to day activities of the business units. The process includes the setting up of a proper system of internal control, identifying issues and taking remedial actions where required.
- The *second line of defense* comes from the risk management function of the Bank, which is independent of business operations. The risk management unit implements the risk management framework, provides independent oversight over specific board directives and is responsible for regular reporting to the Risk Oversight Committee
- The *third line of defense* is the internal audit function & the compliance testing function which provides an independent assessment(s) of the adequacy and effectiveness of the overall risk management framework and governance structures. The internal audit function & compliance testing function report directly to the Board Audit Committee & Compliance Committee.

The PNB Board Risk Oversight Committee (ROC) is mandated to set risk appetite, approve frameworks, policies and processes for managing risk, and accept risks beyond the approval discretion provided to management.

The risk management policy includes:

- a comprehensive risk management approach;
- a detailed structure of limits, guidelines and other parameters used to govern risk-taking;
- a clear delineation of lines of responsibilities for managing risk;
- an adequate system for measuring risk; and
- effective internal controls and a comprehensive monitoring & risk-reporting process

While the first line of defense in risk management lies primarily on the bank's risk taking units as well as the bank's support units, the Risk Management Group is responsible for the monitoring of bank's overall risk management functions to ensure that a robust risk-oriented organization is maintained. The Risk Management Group (RMG) is independent from the business lines and is organized in 7 divisions: Credit Risk Division, ICAAP & BASEL Implementation Division, Market & ALM Division, Operational Risk Division, Information Security and Technology Risk Division, Trust Risk Division and Business Intelligence & Data Warehouse Division.

Each division monitors the implementation of the processes and procedures that support the policies for risk management applicable to the organization. These policies clearly define the kinds of risks to be managed, set forth the organizational structure and provide appropriate training necessary to manage and control risks. The policies also provide for the validation, audits & compliance testing, to measure the effectiveness and suitability of the risk management structure. RMG also functions as the Secretariat to the Risk Oversight Committee which meets monthly to discuss the immediate previous month's total risk profile according to the material risks defined by the bank in its ICAAP document. Further, each risk division engages with all levels of the organization among its business and support groups, including domestic/overseas branches and domestic/foreign subsidiaries. This ensures that the risk management and monitoring is embedded at the moment of origination.

THE BANK'S RISK APPETITE, THRESHOLD & TOLERANCE

The Bank's principle on risk appetite is expressed as Risk Threshold (as defined in the bank's ICAAP document), and is embedded in the business units. Risk Threshold emphasizes that ***"the risk appetite should not go beyond the Bank's capacity to manage risk, thus risk management is the responsibility of everybody"***.

The bank expressed its overall **risk appetite** through the quantitative statement on materiality defined as our **Risk Threshold**. This is the guiding principle behind the execution of our business objectives and is closely monitored alongside the set limits by the various revenue generating groups.

Risk tolerance is expressed in limits (internal & regulatory) for each of the determined material risks, which are more conservative than regulatory limits to provide cushion/buffer.

The following major limits (among others) are set:

1. Earnings At Risk
2. Value At Risk
3. Capital Adequacy Ratio Threshold Level
4. Credit Concentration Limits
5. Single Borrower's Limit

The Board of Directors and Senior Management are responsible in ensuring that the Group maintains at all times the desired level and quality of capital commensurate with the inherent risks (credit, market and operational risks) and with the material risks such as Legal, Compliance, Information Technology/ Security, Strategic Business, Customer Franchise/Reputational that the Group is exposed to.

The Board Risk Oversight Committee (ROC), as delegated by the Board, supported by Risk Management Group, oversees the risk profile and approves the risk management framework of PNB and its related allied subsidiaries.

The Board Policy Committee (BPC) reviews, evaluates, approves and/or endorses for Board approval policies, procedures and manuals of products and services to be offered to the Bank's domestic and overseas market, as well as, Annual Strategic Forecasts, Plans and Budget. They are also responsible in determining the Bank's risk appetite and set limits on risk taking activities and the periodic review of the Bank's ICAAP program.

The Executive Committee (ExCom) reviews, discusses, notes, endorses and/or approves management proposals on credit facilities; investment in financial assets; and borrowings and capital raising, updates and reports on credit, transactional, administrative and other matters.

The Capital Management Sub-Committee of the Asset/Liability Committee (ALCO) is tasked to specifically handle policies and procedures pertaining to the capital planning and assessment as well as possible equity investments of the Bank.

The Senior Management Team and the Business Units agree on the target risk profiles defined by the Bank's strategic plan, and allocate capital based on the risk/return profile. Corporate Planning Group (CorPlan) and RMG monitor this jointly.

RISK CATEGORIES AND DEFINITIONS

Under the Bank's ERM framework, all the risk taking Business Units of the Bank, including its domestic and foreign subsidiaries, shall perform comprehensive assessment of all material risks.

The identification of risks revolves around the monitoring of the risk categories as defined by BSP for supervision purposes. These key risks, namely, credit, market, interest rate, liquidity, operational, compliance, strategic, and reputational risks, are not only monitored under their separate and distinct components, but also monitored across all interrelated business risks. In addition, the various business units identify, measure, monitor and control additional risk categories that may be relevant to their specific areas and correspondingly identify the priorities in the roll up of the bank's Risk & Control Self-Assessment (RCSA) Process.