	competition, regulations, legal, client acceptability, profitability – are taken into account.	engaged in coordinating with the various business sector heads in achieving the bank's business plan. Further, a Product Committee composed of senior managers has been convened and meets regularly to ensure that business environment is closely monitored as to competition; delivery channels and over all service levels are kept at acceptable levels.
Information Technology Risk	Information Technology Strategic Plan is formulated in line with the overall bank's business plan. This is formalized via the approval channel – Board IT Governance Committee and Board of Directors. Enterprise Project Management (EPMF) Framework for technology driven Projects where both the business, technology and support groups are involved	The Bank has institutionalized and implemented the board-level IT Governance Committee which is composed of members of the senior management team, who discuss the monthly ITG. Further, the Bank has formalized the Project Implementation Process (through the EPMF for defined systems implementation to include among others the creation of a PROJECT STEERING COMMITTEE to oversee the project's progress and to ensure that the project's objectives are achieved.
Information Security Risk	Enterprise Information Security Policies, the cornerstone of the Bank's information security management system, is a component of an effective Corporate Governance. This communicates Management's directives and support for PNB's information security programs and strategies. The high level security policies stated herein are based on International Organization for Standardization (ISO) 27000 series of internationally-accepted information security and risk management standards, related laws and regulations.	Adoption of globally accepted ISMS (Information Security Management System – in compliance with BSP Circulars and ISO mandated functions) – is continuously reviewed and revised as necessary to ensure that the bank's information assets are duly protected and that the risk of theft, leakage and fraud are minimized, and/or eliminated.
Business Continuity Risk	Business Continuity Program – administered throughout the organization where each business unit formulates individual BCP.	a) Call Tree Program (a component of the BCP) is administered throughout organization to ensure that each personnel stays connected when an emergency situation arises from natural and man-made disasters b) Business Impact Analysis – is accomplished on a regular basis to provide a central forum of prioritizing services whenever an emergency situation arises c) BCP Technical Tests are done on an annual basis to determine readiness of the bank's applications and system for continued delivery of prioritized services

Note: The Bank applies the same risk management policy for both the Bank and its subsidiaries and affiliates as a Group.

(c) Minority Shareholders

Indicate the principal risk of the exercise of controlling shareholders' voting power.

Risk to Minority Shareholders
Stockholders holding or representing at least two thirds (2/3) of the outstanding capital stock of the corporation may control the vote for matters such as the amendment of articles of incorporation, removal of directors, shorten or extend corporate term, increase or decrease capital, sale or other disposition of assets, invest corporate funds in another corporation or business or for any other purpose, declaration of dividends, merger or consolidation, voluntary dissolution, etc.

3) Control System Set Up

(a) Company

Briefly describe the control systems set up to assess, manage and control the main issue/s faced by the company: