		its predictive ability. c) Reporting System Effective Management Information System (MIS) are in place and, at a minimum, has the capacity to capture accurate credit risk exposure/position of the Bank real time. A monthly credit dashboard is used as the reporting tool for appropriate and timely risk management process. d) Remedial Management System Work-out system for managing problem credits are in place. Among others, these are renewals, extension of payment, restructuring, take-out of loans by other banks; and regular review of the sufficiency of valuation reserves. e) Event-Driven Stress Testing Techniques are conducted to determine the payment capacity of affected borrowers' accounts. A Rapid Portfolio Review program is in place to quickly identify possible problem credits on account of evolving events both domestic and global. Results of the stress testing shows minimum impact and have no material effect to Bank's NPL ratio and CAR.
Operational Risk		
People Risk	a) In PNB operational losses may be attributed to human error which can be brought about by inadequate training and management. b) Further, there is the risk of "non-fit" personnel being "forced" to occupy positions that they are not qualified for.	a) This issue is being addressed through formal (continuously conducting trainings) or informal (monthly meetings and discussing issues at hand) means. These trainings also address the issue of relying on key performers instead of cross training each team member. b) Annual evaluation and the implementation of balanced scorecards are used to ensure that ill-fitted personnel are either re-trained, re-tooled and re-skilled to equip them better.
Process Risk	Most processes are designed with audited fail-safes and checking procedures. Since processes interact with other risky variables - the external environment, business strategy and people – it is difficult to sound the all clear. However, processes can make an institution vulnerable in other ways.	The Bank has documented policies and procedures duly approved by the Board. The Internal Audit Group as well as the various officers tasked with the review function regularly monitors the implementation of these documented policies and procedures.
Business Strategy Risk	Strategic Risk can arise when the direction/strategy of the bank can lead to non-achievement of business targets. This results in a new focus of a business sector without consolidating this with the bank's overall business plan and strategy.	At PNB, strategic risk is managed through each business sector performing "actuals vs targets" sessions with and report to the Board of Directors through regular Management Profitability Reporting Sessions. In addition, the coordination between business sectors are done through regular meetings by the senior management team to ensure that overall business targets are continually revisited.
Business Environment Risk	Banks tend to have the least control over this source of operational risk yet it still needs to be managed. Business environment risk can arise from unanticipated legislative changes such as consumer affairs, physical threats such as bank robberies, terrorist attacks, natural disasters and regulatory required financial report changes, new or otherwise. New competitive threats such as faster delivery channels, new products, new entrants and the ever-increasing rationalization of the banking industry are driving banks to become much more	At PNB, we have become fully involved and engaged in the Product Management Business Framework where old and new products alike are monitored by assigned product managers who coordinate 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.

	nimble-footed. The flexibility required to remain in the game leads some banks to take shortcuts that eventually expose them to some new source of operational risk.	
Information Technology Risk	The growing dependence of financial institutions on IT systems is a key source of operational risk. Data corruption problems, whether accidental or deliberate, have been sources of embarrassing and costly operational mistakes. Losses may also result from a simple change in program, which end up being incorrectly tested prior to cut-over to production.	The Bank has institutionalized and implemented the IT Governance Committee which is composed of members of the senior management team, who discuss the monthly ITG Dashboard prior to it being presented to the Risk Oversight Committee with following focused topics: a) Bank's IT Strategic Plan b) Incident Reporting c) Business Continuity Management d) Major IT Projects e) Enterprise Project Management Further, the Bank has formalized the Project Implementation Process 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	IS Risk is assessed as the unwanted or unintended negative impact or consequence to the bank as a result of exposure to vulnerability or threat to the bank's information assets.	Adoption of risk mitigation and management tools as follows: a) Regular Vulnerability and Penetration Testing b) Increased Risk Awareness Campaign c) Tight Data Protection and Incident Management Reporting & corresponding Resolution Program d) Consistent Patch Management Program to prevent External and Internal Attacks e) Regular review of the Business Impact on security threats
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

(b) Group

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

Note: The Bank applies the same risk control systems set up for both the Bank and its subsidiaries and affiliates as a Group.

(c) Committee

Identify the committee or any other body of corporate governance in charge of laying down and supervising these control mechanisms, and give details of its functions:

Committee/Unit	Control Mechanism	Details of its Functions
Risk Oversight Committee (ROC)	a) Approval of risk limits such as Value at Risk limits, Stop loss limits, credit risk factors, liquidity gap limits, earnings at risk limit.	Functions: The BSP-mandated functions of the ROC are as follows: