

	group or conglomerate where the financial institution belongs.		
Included in the Operational Risks:			
Customer Franchise & Reputational Risk	<p>Reputational risk is the current and prospective impact on earnings or capital arising from negative public opinion.</p> <p>Customer franchise risk is defined as the failure to find, attract, and win new clients, nurture and retain those the Bank already has, and entice former clients back into the fold as well as the failure to meet client's expectation in delivering the Bank's products and services.</p>	<ul style="list-style-type: none"> ▪ Risk Identification ▪ Risk Measurement ▪ Risk Measurement ▪ Risk Evaluation (i.e. Analysis of Risk) ▪ Risk Management (i.e. Monitor, Control or Mitigate Risk) <p>Monitoring of Pillar II Risks fall under the purview of Operational Risk Management:</p> <ul style="list-style-type: none"> ▪ Risk Identification – Risk Maps ▪ Risk Measurement and Analysis – ICAAP Risk Assessment 	<ul style="list-style-type: none"> ▪ Account Closures Report ▪ Service Desk Customer Issues Report/Customer Complaints Monitoring Report ▪ Mystery Caller/Shopper ▪ Evaluation/ Risk Mitigation of negative media coverage ▪ Public Relations Campaign ▪ Review of Stock Price performance ▪ Fraud Management Program
Strategic Risks	<p>Strategic business risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.</p>	<p>Major Factors Considered:</p> <ul style="list-style-type: none"> ▪ Products ▪ Technology ▪ People ▪ Policies and Processes ▪ Stakeholders (including customer and regulators) 	<ul style="list-style-type: none"> ▪ Management Profitability Reports ▪ Benchmarking vis-a-vis Industry, Peers ▪ Economic Forecasting
Information Technology and Information Security Risk (includes Core Banking Implementation Risk)	<p>Information Technology Risk is a business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within the Bank (ISACA Risk IT Framework). IT Risk results to Information Security Risk since the risk would somehow result to non-</p>		<ul style="list-style-type: none"> ▪ Risk Asset Register ▪ Incident Reporting Management ▪ Information Security Policy Formulation ▪ Project Management Framework ▪ Risk Assessment ▪ Project Progress Reporting ▪ Approvals for

	<p>preservation of any or all of the domains of information security; that is, confidentiality, integrity and availability of information asset (NIST IR 7298 Revision 2).</p> <p>Technology Integration risk is another aspect and is defined as the negative impact on the organization for the possible delay or failure of the institution to integrate its various systems application, such as the Core Banking implementation. It also includes the risk of delay in appropriate servicing of clients requirements to maintain competitiveness in the market.</p>		<p>major scope changes</p> <ul style="list-style-type: none"> ▪ Risk Assessment for new/upgrade of information / automated systems ▪ Harmonization Timeline Tracking
<p>New Regulations Risk</p>	<p>New Regulations Risk is the current and prospective risk to earnings or capital arising from highly regulated jurisdiction and when rules and regulations are constantly changing. It is an important qualitative risk which must be monitored and managed, as regulatory sanctions from non-compliance, especially in extreme cases, may involve not just mere loss of reputation or financial penalties, but in extreme cases, a revocation of the banking charter or franchise (BAP Risk</p>		<ul style="list-style-type: none"> ▪ Risk Asset Register ▪ Incident Reporting Management ▪ Information Security Policy Formulation ▪ Project Management Framework ▪ Risk Assessment ▪ Project Progress Reporting ▪ Approvals for major scope changes ▪ Risk Assessment for new/upgrade of information / automated systems ▪ Harmonization Timeline Tracking