RISK MANAGEMENT

For a financial services company such as SAIB, operating in today's global business environment, requires a careful identification of the different types of risks, managing the risks, and balancing risk and return. This includes efficient allocation of regulatory capital to support healthy balance sheet growth. Being a custodian of customer deposits, the Bank has to apply best in class risk management practices in order to safeguard the interests of customers, investors and other stakeholders. Hence, the Bank has a well-defined and documented risk management framework in place to prudently fulfil its role as a custodian and intermediary, as well as to rigorously comply with regulatory requirements.

At the apex of the risk policies and procedures of the Bank is the Risk Management Policy Guide, prepared in conformance with the requirements of the Saudi Arabian Monetary Authority (SAMA). This describes in detail the risks the Bank is exposed to and the policies and mechanisms in place to measure, manage and control the risks. Some of the main governance manuals developed for this purpose are the Risk Appetite Framework (RAF), Credit Policy Guide and Treasury Policy Guide.

The RAF is the cornerstone of the Bank's risk management and is overseen and approved by the Board of Directors. It monitors and measures risk tolerance in a structured and transparent manner and infuses risk management considerations into the Bank's strategy and operations. The Board is supported by the Board Risk Committee which recommends policies for Board approval and oversees key risks within the Bank. There are also several supporting committees at Management level including the Enterprise Risk Management Committee, the Credit Committee and the Asset and Liability Committee. At the Departmental level, the Bank has a Risk Management Group headed by the Chief Risk Officer.

The RAF is aligned with the Bank's strategic planning, business planning, capital planning and policies and documents issued by the Board of Directors. The RAF sets out the nature of risks arising from the Bank's strategy. It defines the maximum level of risk the Bank could take without hampering its operations (risk capacity); the maximum level of risk the Bank is willing to take (risk appetite); maximum level of other quantifiable risks (other risk limits); and the desired risk-return trade-off.

In addition to the RAF, the Board has also approved the Risk Assessment Policy Guide which includes the Risk Appetite Policy Framework, Credit Policy Guide, Treasury Policy Guide, Stress Test Policy, Internal Capital Adequacy Assessment Plan Policy, Operational Risk Policy, Fraud Risk Policy, Information Security Policy among others. The Board is also responsible for approving and implementing policies to comply with SAMA guidelines, accounting and reporting standards (including IFRS 9 in relation to anticipated credit loss provisioning) and best industry practices such as Basel guidelines. A comprehensive Group IFRS 9 Governance Policy Framework was approved in 2018. This is backed by additional Management level policies such as the IFRS 9 Data Management and Control Framework Policy and the IFRS 9 Governance Framework.

In addition to the above, the Bank's Internal Audit Function reports to the Audit Committee of the Board of Directors and conducts an independent validation of compliance with risk policies and procedures and the adequacy and effective of the risk management framework. This reflects the "three lines of defence" risk management approach adopted by the Bank, whereby the front line business units are made risk aware, the support functions such as the Risk Management Group are an important second line of defence, and Internal Audit is the third line.

A description of the different types of risks the Bank is exposed to and how the Bank manages these risks is given below:

Credit risk

This is the risk of loss occurring due to counterparties in credit transactions not fulfilling or only partly fulfilling their financial obligations. The credit risk may arise from loans, advances, guarantees, derivatives and foreign exchange products. Credit risk is assessed by a comprehensive framework including an independent credit risk review and credit monitoring process. The Credit Policy Guide (CPG) contains guidelines for the process. The CPG seeks to maximise return while recording, managing and mitigating the associated risks. The Probability of Default (PD) is assessed using internal rating tools. External ratings from major rating agencies are also used when they are available.

The Bank is improving the credit management process by further developing the post-sanction review process to mitigate potential credit losses that may arise.

Operational risk

This is the risk arising from failures in systems, internal processes, human error or external events. The Bank's Operational Risk Management Framework defines the various types of operational risk, and how they are to be assessed and controlled. The assessment and control of operational risks in all organisational units of the Bank are monitored through Risk Control Self Assessment (RCSA) exercises, and establishing a Bank-wide Operational Risk Appetite Matrix. Operational risk losses are monitored on an ongoing basis and corrective action is taken.

Liquidity risk

This is the risk that the Bank will have inadequate funds, or lack funds at an acceptable cost, to meet its obligations when needed. A cause of liquidity risk can be credit downgrades or market disruptions which can make unavailable previously expected sources of funds. The Bank carefully monitors its liquidity position on a daily basis to minimise liquidity risk. Several ratios including the Daily Liquidity Ratio are monitored for this purpose and kept within SAMA guidelines. Liquidity stress testing is also carried out under both normal and stressed scenarios.

Market risk

This is the risk that the fair values of future cash flows of financial instruments will fluctuate due to changes in market variables such as interest rates, exchange rates and equity prices. Measures to manage such risks are laid down in the Treasury Policy Guide issued by the Board of Directors.

Commission rate risk

This is the risk that changes in commission rates will affect either the fair values or future cash flows of financial instruments. This could arise from timing differences in fixed and floating rate assets and liabilities. The Board has set commission rate gap limits by time periods. The Bank also uses hedging strategies to minimise risk within time limits.

Currency risk

This is the risk of changes in exchange rates having an impact on financial position or cash flows. The risk is minimised by limited foreign currency exposure, setting limits on forward maturity gaps and by hedging strategies.

Equity price risk

This is the risk of changes in the value of the Bank's investment portfolio due to fluctuations in prices of equities or market indices. The Board sets limits on exposure to individual industries and for the overall exposure.

Financial crime risk

This is the risk of losses due to frauds and other crimes which are a significant risk for banks as well as their staff. The occurrence of such crimes can have a very negative impact on the reputation of the Bank. SAIB has continued developing its anti-financial fraud control system.

Cyber information security risk

As technology develops it brings with it associated risks. Today cyber risks are an ever-present threat for all financial institutions. The Bank is extremely vigilant in this area; it has deployed precautionary measures including 24x7 Security Operation Centre, Vulnerability Management Programmes and Attack Simulation Exercise to enhance Cyber Resilience. Security practices and culture have also been reinforced through various programmes to educate staff. The Information Security and Operations Risk Division commenced implementation of its new strategy for 2018-2020 which was approved by the Information Security Committee. Confidentiality, integrity, privacy and access controls were integrated into all business and technical processes. Though there have been cyber attacks targeting the Middle East and Saudi Arabia, the Bank has shown resilience in withstanding them.

Risk-based security audit conducted by internal audit, external agencies and certification bodies including ISO 27001 (Information Security Management System) were completed with satisfactory findings. Conformance with international standards and best practices such as General Data Protection Regulation have been verified and assured. In addition, the Information Security and Operation Risk Division complies with the Saudi Information and Cyber Security Regulations imposed by Saudi National Cyber Security Authority (CSA) and SAMA.

Business continuity plan

The Bank continued to recognise the importance of this area and make progress in it in 2018. A robust Business Continuity Plan (BCP) will enable the Bank to respond to a serious disruptive incident in a timely and appropriate manner. During 2018, comprehensive tests were conducted on two separate occasions. In addition, a continuous five-day recovery test was conducted on all mission-critical IT operations by switching them to operate from the Bank's Disaster Recovery Centre (DRC). The Bank will continue to upgrade its disaster recovery capabilities by switching operations in this manner in the event of a major incident. This needs to ensure that they can operate independent of the primary site. The Bank is in the process of establishing a new DRC which will be ready in 2019. Continued training on business continuity will be conducted. The Bank maintained the ISO 22301 Certification for Business Continuity Management through validation by an independent authority.