GRI 102-11

Risk Management

As a financial services company operating in today's interconnected global business environment, it is more important than ever for SAIB to identify and understand the different types of risks it faces and how to manage them, and balance risk and return. SAIB has to apply best-in-class risk management practices to safeguard the interests of its customers, investors, and other stakeholders and efficiently allocate regulatory capital to support healthy balance sheet growth. To this end, SAIB has a comprehensive risk management framework to support the Bank in its role as custodian and intermediary, and to comply with regulatory requirements.

The Bank's Risk Management Policy Guide conforms with the requirements of the Saudi Arabian Monetary Authority (SAMA). The Policy details the risks the Bank is exposed to and the policies and protocols in place to measure, manage, and control the risks.

The Risk Appetite Framework (RAF) is the basis for the Bank's risk management, overseen and approved by the Board of Directors. The Framework presents a structured and transparent process for monitoring and measuring risk tolerance and incorporates risk management considerations into the Bank's strategy and operations. The Board Risk Committee supports the Board of Directors by recommending policies and overseeing key risks within the Bank. In addition, there are several supporting committees at Management level – 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 to the Bank's strategic planning, business planning, capital planning, and policies and documents issued by the Board of Directors. The RAF lays out the risks that arise from the Bank's strategy and defines the following:

- Risk capacity: The maximum level of risk the Bank can assume without affecting operations
- Risk appetite: The maximum level of risk the Bank is willing to undertake
- Other risk limits: The maximum level of other quantifiable risks
- Desired risk-return trade-off.

The Board has also approved the Risk Assessment Policy Guide which includes (but is not limited to) the following:

- Risk Appetite Policy Framework
- Credit Policy Guide
- Treasury Policy Guide
- Stress Test Policy
- Internal Capital Adequacy Assessment Plan Policy
- Operational Risk Policy
- Internal Liquidity Adequacy Assessment Plan: a new framework to ensure prudent liquidity management versus the asset maturity profile
- Information Security Policy

The Board is 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 the Basel guidelines. A comprehensive Group IFRS 9 Governance Policy Framework was approved in 2018, backed by additional Management level policies including the IFRS 9 Data Management and Control Framework Policy and the IFRS 9 Governance Framework.

Furthermore, the Bank's internal audit function reports to the Audit Committee of the Board of Directors and independently validates compliance with risk policies and procedures and the adequacy and effectiveness of the risk management framework. This is the "Three Lines of Defence" risk management approach of the Bank, which sees the frontline business units are made risk aware, the support functions such as the Risk Management Group are the Second line of Defence, and Internal Audit is the Third line of Defence.

The different types of risk the Bank is exposed to and the measures the Bank takes to manage these risks are discussed in further detail below.

Credit risk

Credit risk is the risk of loss occurring when counterparties in credit transactions do not fulfil or only partly fulfil their financial obligations. Loans, advances, guarantees, derivatives, and foreign exchange products are all subject to credit risk. A comprehensive framework is in place for assessing credit risk, including an independent credit risk review and credit monitoring process. The Credit Policy Guide (CPG) contains guidelines for the process and seeks to maximize return while recording, managing, and mitigating the associated risks. The Probability of Default (PD) is assessed using internal rating tools and external rating from major rating agencies are also used where available.

SAIB continues to improve the credit management process by further developing the post-sanction review process to alleviate potential credit losses that may arise.

Operational risk

Operational risk arises from failures in systems, internal processes, human error, or external events. The Bank's Operational Risk Management Framework lays out the various types of operational risk and how to assess and control them. Assessment and control of operational risks across all organization units of the Bank are monitored via Risk Control Self-Assessment (RCSA) exercises and a Bank-wide Operational Risk Appetite Matrix. Operational risk losses are continuously monitored, with corrective action taken as necessary.

Liquidity risk

Liquidity risk is the risk where the Bank is unable to meet its obligations due to having inadequate funds or access to funds at an acceptable cost. Liquidity risk can be caused by credit downgrades or market disruptions which can render unavailable previously expected sources of funds. The Bank monitors its liquidity position daily to minimize liquidity risk and monitors several ratios including the daily Liquidity Coverage Ratio (LCR) and the Net Stable Funding Ratio (NSFR) which measures the funding of long term assets, ensuring they are within SAMA guidelines. The Bank also carries out liquidity stress testing under both normal and stressed scenarios.

Market risk

Market risk is the risk that the fair values of future cash flows of financial instruments fluctuate due to changes in market variables such as interest rates, exchange rates, and equity prices. The Treasury Policy Guide issued by the Board of Directors lays out measures to manage such risks.

Commission rate risk

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

Currency risk

Currency risk is the risk of changes in exchange rates affecting the Bank's financial position or cash flows. This risk can be minimized by limited foreign currency exposure, setting limits on forward maturity gaps, and by hedging strategies.

Equity price risk

Equity risk is the risk of changes in the value of the Bank's investment portfolio as a result of fluctuations in prices of equities or market indices. The Board sets limits on exposure to specific industries and for the overall exposure.

Financial crime risk

Financial crime risk arises from the risk of losses due to frauds and other crimes which pose a significant risk to banks and their staff. Such crimes can have a negative impact on the reputation of the Bank. SAIB continues to develop its anti-financial fraud control system to mitigate risks.

Cyber information security risk

Cyber risks are a significant threat for all financial institutions and SAIB is extremely vigilant in this area. Precautionary measures taken by the Bank include the 24x7 Security Operation Centre, Vulnerability Management Programmes, and Attack Simulation Exercises to enhance resilience to cyberattacks. Programmes to educate staff help to reinforce the culture and security practices in place. The Information Security Committee approved the implementation of a new strategy by the Information Security and Operations Risk Division for 2018-2020. Confidentiality, integrity, privacy, and access controls have been integrated into all business and technical processes. Moreover, the Bank has shown resilience in withstanding cyberattacks that have targeted the Middle East and Saudi Arabia.

Risk-based security audits conducted by internal audit, external agencies, and certification bodies such as ISO 27001 (Information Security Management System) have been completed with satisfactory results. The Bank's conformance with international standards and best practices such as the General Data Protection Regulation has been verified and assured and the Information Security and Operation Risk Division complies with the Saudi Information and Cyber Security Regulations imposed by the Saudi National Cyber Security Authority (CSA) and SAMA.

Business Continuity Management (BCM)

A strong Business Continuity Plan (BCP) is a priority for SAIB and the Bank continued to develop this in 2019. The BCM enables the Bank to respond to disruptive incidents quickly and effectively with minimal downtime. The Bank conducted comprehensive tests during the year and continued to upgrade the capabilities of its Disaster Recovery Centre (DRC). Additionally, the Bank's ISO 22301 Certification for Business Continuity Management is being upgraded for the new version by an independent authority.