Commercial banks in Saudi Arabia are well capitalized to withstand any downturn in business cycle. Average Capital Adequacy Ratio (CAR) was in excess of 17% which is almost double compared to the recommended 8% from BASEL ΙΙ. The CAR of the listed banks range from 14% to 19% and 8 out of 10 listed banks have total capital ratio in excess of 17%. Moreover, Tier Ι capital ratios are also high for the entire banking system. Overall credit ratings of the banking system are high with majority of them having high ratings due to strong fundamentals.

**Alrajhi** **Bank** recognises the importance of an effective risk management and control measures to ensure the Bank’s corporate value, sustained profitability and continued enhancement of shareholder value.

## The management of operational risk is an important priority for Alrajhi Bank. Alrajhi has established within its risk management framework a holistic risk management governance structure for risk management which balances risks and returns, as well as integrated risk management processes for operational risk.

Alrajhi seeks to meet the standards and expectations of regulatory authorities through a number of initiatives and activities to support compliance with regulations governing anti-money laundering and counter financing of terrorism. To further enhance operational risk management in response to threat of external fraud, losses arising from frauds or control lapses are analyzed in depth to identify the causes of such losses and to implement remedial actions to prevent recurrence. Analyses of impaired financing attributed to operational lapses are also conducted diligently and the findings are disseminated to all business units as learning points. The bank manages its outsourcing activities through the Guidelines on Outsourcing Activities which stipulate the requirements and the operating procedures to be observed in managing activities that are outsourced to third party service providers. This is to ensure that the risks associated with outsourcing activities are managed effectively. Basel II - Pillar 3 Disclosure As at 30 June 2015.

Disaster recovery and business continuity plans are put in place as an integral part of the bank’s strategy to mitigate risk and manage the impact of loss events. Where appropriate, the bank mitigates risk of high impact loss events by relevant insurance coverage. The bank protects and ensures information security through continuous assessment of the security features on all computer platforms and network infrastructure, and implementation of appropriate security controls to protect against the misuse or compromise of information assets. In addition, Alrajhi continues to undertake initiatives to maintain 100% systems availability and robust system performance in the bank’s computer systems, peripherals and network infrastructure to ensure uninterrupted transmission.

**In Alrajhi bank**, the risk management processes encompass four broad processes, namely risk identification, risk assessment and measurement, risk control and mitigation and risk monitoring. Stress test and scenario analysis serve as important risk management tools as part of the Bank's risk assessment process and are used to assess the financial risks and management capability of the Bank to continue to operate effectively under different stressed scenarios. The stress test and scenario analysis will assist the Bank in the following:

1. Evaluating the optimal capitalisation level for the Bank to weather extreme banking scenarios.
2. Understanding the nature and key risk profile of the Bank;
3. Estimating the adequacy or liquidity contingency planning; and
4. Assessing the effectiveness of risk mitigation which are already established.

To further enhance operational risk management in response to threat of external fraud, losses arising from frauds or control lapses are analyzed in depth to identify the causes of such losses and to implement remedial actions to prevent recurrence. Analyses of impaired financing attributed to operational lapses are also conducted diligently and the findings are disseminated to all business units as learning points.

**To mitigate** operational risk, Alrajhi bank uses various tools including:

• Risk and Control Self-Assessment (RCSA) – to enhance management assessment of the state of the risk and control environment.

• Key risk indicators – to collect statistical data on an ongoing basis to facilitate early detection of Key operational risk and control deficiencies

• Operational risk incident reporting and data collection – to facilitate an enhanced analysis and timely reporting of operational risk data which are useful in assessing the bank’s operational risk exposure and in strengthening the internal control environment

The bank’s employs the following key methods to mitigate its operational risk:

• System of internal controls based on segregation of duties, independent checks, segmented system access control and multi-tier authorization processes.

• Documented operational risk management policies and procedural manuals to mitigate errors by users.

• Processes to ensure compliance with internal policies, guidelines, controls and procedures and appropriate punitive actions are taken against errant staff.

• Periodic review and enhancement of operational risk limits and controls strategies.

• Disaster recovery and business continuity plans put in place to mitigate risk and manage the impact of loss events.

• Insurance coverage to mitigate risk of high impact loss events, where appropriate

• Review of outsourcing activities to ensure that services providers adhere to the terms and conditions in the service agreement and that their integrity and service quality are not compromised. Basel II - Pillar 3 Disclosure As at 30 June 2015.

Reporting forms an essential part of operational risk management. Alrajhi bank’s risk management processes are designed to ensure that operational issues are identified, escalated and managed on a timely manner. Operational risk areas for the key business and control units are reported through monthly operational risk management reports, which provide analyses and action plans for each significant business operation. The operational risk areas considered include premises controls and safety, losses due to fraud or control lapses, system availability, disaster recovery and business continuity plan simulations, outsourcing activities and legal actions taken against the bank. The operational risk management reports are tabled to the ORC and the ERMC for deliberations.