INFORMATION TECHNOLOGY REPORT

The financial and technology landscapes have been transformed markedly in recent years against the backdrop of a highly competitive environment.

Emphasis has been placed on revenue generation, the reduction of costs, innovation of products and services, improved customer service and the realisation of organisational efficiencies and investments, whilst also reinforcing robust governance principles on an on-going basis.

The congruency of the financial and technological elements and their inherent inter-dependencies are starkly noticeable, with the properties of information technology bearing considerable influence over organisational strategies, contemporary challenges and sustainable growth. Both group and bank, being at the forefront of their core business, recognise these properties and the benefits associated with harnessing them to leverage internal cross-sectional advantages, whilst ensuring the bank remains competitive. There exists an ability to adapt dynamically to market changes, meeting the broader strategic objectives of a complex business and technology environment. In this regard, the bank ably responded to market needs, implementing systems integrated into the current core banking environment to address global trading capabilities, the latter representing a turning point in the positioning of the bank. A further milestone was achieved when the bank's portfolio of products and services was broadened to include cheque accounts. The externally-hosted system which facilitates the cheque account product is an extension of the electronic banking system environment.

In other developments, customer service improvement and processing efficiencies were targeted, resulting in the streamlining of certain applications and processes, including the enhancement of the Credit Application Processing System (CAPS). The introduction of IT3B Statements as part of the bank's 24/7 Online Statement System, which enables secure customer access via the internet, led to further efficiencies from a customer services perspective. On the hard technology front, several older PABX units located at branches were upgraded to renew and expand customer communication requirements, with an opportunity to standardise technologies adopted. From a networking infrastructure perspective, the bank's existing data network was extended to incorporate the strategically positioned Killarney Mall business office, with its relatively low system and technology dependencies at this stage.

Broadly, however, the increased portfolio of products and services, coupled with the incremental growth and strategic positioning of the business, is anticipated to create an increased dependency on underlying networks, systems and technologies adopted. It will, therefore, be essential to acquire supplementary technologies, including replication mechanisms to ensure the high availability of critical business systems, for continuity purposes. As a growing organisation, the bank recognises the value of business process re-engineering initiatives and, accordingly, plans to engage the creativity of its key resources to refine and automate processes wherever possible, create business intelligence information stacks and maximise the use of existing technologies, which are targeted contributors of greater efficiencies, lower costs and increased benefits for all stakeholders.

Looking ahead, the bank seeks to explore mobile banking solutions to encourage innovative, cross-platform user delivery and consumption channels, whilst garnering the attractiveness of social media integration to stimulate consumer responsiveness. We now look to bold initiatives, capitalisation on existing investments and the leveraging of technologies which promote an optimistic outlook. We believe it prudent to take cognisance of a constantly evolving and sophisticated security landscape and, with this in mind, the hardening of appropriate security monitoring and enforcement mechanisms, supplemented by sound governance principles and controls, will assist in bolstering the barriers to a variety of technology threats and risks. In line with this, the introduction of the Protection of Personal Information Act is a welcome measure to reinforce appropriate layers of information security standards, benefiting customers and financial institutions alike.

Business Continuity and Disaster Recovery Report

The board of directors and management of Al Baraka Bank recognise that our financial institution is not immune to business disruptions arising from the effects of suspended operations which are the result of natural disasters, systems failures, power outages and similar events.

We are aware that such disruptions could have dire consequences on the bank's activities insofar as its business operations, public image and reliability of services are concerned. In an effort to minimise disruption to the continued activities of the bank, the risk and capital management committee of the board, together with management, has ensured the compilation and update of individual business continuity plans in terms of each business unit and the bank as a whole, taking into consideration the following essential components:

- The continuation of minimum, but indispensable banking services during and after a disaster;
- The provision of alternative communications with relevant stakeholders, including customers, employees, directors and regulators;
- The identification of alternative physical locations for employees and/or customers;
- The continuation of banking business with critical suppliers, contractors and other banks; and
- Compliance with regulatory reporting.

Relevant business continuity plans have been compiled to address failures which impact on information technology systems, as well as on the individual business units and branches. In this regard, the bank's recovery objectives are designed to ensure:

- That critical personnel are available and are on stand-by to manage the disruption;
- The continuation of critical operations and services with minimum disruption during or after a disaster;
- That the likelihood of impact of risks resulting from disruption is minimised; and
- That the level of recovery and complete banking services are quickly attained.

In the event of an off-site recovery being necessitated through the complete or partial loss of premises or loss of information technology systems or a combination thereof, the bank has access to five fully equipped disaster recovery centres located within South Africa. Each comprises secure off-site facilities with a range of dedicated high-performance servers, desktop computers and networking equipment, as well as desk and seating arrangements, printing and telephony services, access to general amenities and access to professional on-site engineers.

In terms of data strategy, the bank utilises the services of recognised off-site storage facilities nationally to store back-up tapes, whilst on-premise tapes pending transit are stored in safes. Back-ups are regularly tested to ensure that data is recoverable and that data integrity is reliable.

The recovery methodology adopted is the simulation of a disaster as close to the real event as possible. This involves performing the necessary recovery processes initially within a controlled environment.

The purpose is to establish the impact of any major variances in the technology and processes, as well as to test the theory of the recovery plans.

Testing of the bank's disaster recovery processes is conducted four times a year, with two tests conducted within the KwaZulu-Natal region, one test in Gauteng and one in the Cape Town region. Each regional test includes a simulated branch recovery, as well as a full recovery at the disaster recovery centre in conjunction with key service providers and external participants. Thus, the recovery efforts represent eight effective tests being conducted per annum, incorporating both off- and on-site branch recoveries per region.

The business continuity plans and disaster recovery processes are reviewed by internal audit on an annual basis, ensuring that these plans and processes remain current and effective. The organisation-wide business continuity plans are stored on a combination-locked flash drive with documents password-protected and under the custody of executives, general managers, branch managers and risk and IT managers.

Finally, the bank recognises the need to facilitate the higher availability of critical business systems, particularly in view of strategic business growth, a broader base of products and services and an increased dependency on the information technology and systems environment.

Accordingly, an investigation into appropriate high-availability system replication solutions to facilitate quicker recovery time-frames is envisaged.