



## Security Assessment and Roadmap for a large Bank in Kingdom of Saudi Arabia

### Client Profile

The client is one of the largest banks in Saudi Arabia and the Middle East, employing over 4,000 people in over 240 branches throughout the Kingdom. The bank has two international branches in Beirut and Bahrain. It has five representative offices across Europe and Asia. Its banking infrastructure includes over 800 Automated Teller Machines and more than 5,000 Point-of-Sale Terminals. The bank operates the largest dealing room in foreign exchange and money markets in the Middle East. Since its inception in 1953, the bank has maintained a successful track record in Saudi Arabia and Middle East.

### Client Context

With the proliferation of security threats through different sources, it was imperative for the bank to have a security strategy. This would enable the bank to combat any security threats that can cause a huge impact on business. The bank wanted to review its existing security infrastructure, assess the vulnerability of IT components and develop enhanced security architecture.

The objective of the bank was:

- To evaluate its compliance vis-à-vis BS 7799 standards
- To establish the ISMS (Information Security Management System) framework aligned with business and IT requirements
- Conduct specific security assessment of selected technology constituents

Microland was chosen for the engagement based on its infrastructure security consulting capabilities, domain expertise and track record.

### Microland Approach

Microland leveraged its extensive experience in the Security Lifecycle Services domain to address the bank's needs. The audit was carried out on an extremely large and complex network with a large suite of technologies deployed across five locations.

A team of expert security consultants worked to deliver an effective and comprehensive solution addressing possible threats. The first step was to develop a risk management

framework specific to the bank after understanding the business and process. Then identify the key IT assets which are critical for banking operations and carry out a Risk Assessment exercise. Microland reviewed the existing security policies, standards and procedures to identify security gaps and define a set of policies and processes in line with the ISMS requirements. Security and Vulnerability Assessment of various IT components was done to identify the vulnerabilities in the IT infrastructure (servers, network equipments etc) and the necessary mitigation strategy defined. Microland developed an ISMS framework and roadmap considering the existing IT strategy and security culture. The framework enabled tracking and managing technology vulnerabilities efficiently. Finally, the Microland team defined the security architecture within the ISSD (Information System Security Division).

### Key Deliverables

- Adherence to BS7799 compliance
- Review and recommend compliance level of current security posture as per BS 7799 standards
- Definition of IT Security Organization Structure and Security Architecture
- Definition of the Information System Security Department (ISSD) structure
- Identification of existing processes and definition of proposed ones
- Suggestions for establishing Incident Management and Monitoring Functions within security organization
- Security and Vulnerability Assessment (and recommendations) of various IT components
- Security Assessment of Internet Banking and core banking application

### Benefits

- Adherence to security standards
- A robust and secure environment for internet based transactions as a result of bridging security gaps identified through assessments
- Effective management of IT infrastructure vulnerabilities using Vulnerability Tracking
- System based on ISMS framework
- Increased level of security awareness across the organization