BANK OF NAMIBIA

CIRCULAR BIA 1/03

TO: ALL BANKING INSTITUTIONS

DATE: 24 SEPTEMBER 2003

ELECTRONIC BANKING

1 Background

As technology has advanced, new banking products and services that are delivered through electronic channels, commonly known as e-banking, have become available. E-banking has many advantages, but also carries several risks. For this reason, the Bank of Namibia requested the banking institutions to complete a survey regarding electronic banking and the attendant risks.

Since the number of customers using e-banking is on the increase, banks need to ensure that risks related to e-banking are managed properly. In July 2003, the Basel Committee on Banking Supervision published the *Risk Management Principles for Electronic Banking*. The principles have been developed to assist banking institutions to expand their existing risk oversight policies and processes to cover their e-banking activities.

2 Implementation

To ensure a high standard of e-banking risk management in Namibia, banking institutions are required to implement the *Risk Management Principles for Electronic Banking* by the end of 2003. The Bank will verify the implementation of the principles during bank examinations and by means of regular surveys regarding electronic banking in Namibia. Banks can obtain a complete copy of the *Risk Management Principles for Electronic Banking* from http://www.bis.org. For ease of reference, the principles as listed in the Basel Committee document are included below.

1. The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.
2. The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.
3. The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.
4. Banks should take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business over the internet.
5. Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.

6. Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.
7. Banks should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.
8. Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.
9. Banks should ensure that clear audit trails exist for all e-banking transactions.
10. Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.
11. Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.
12. Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdiction to which the bank is providing e-banking products and services.
13. Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.
14. Banks should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.

Banks need to comply with the *Risk Management Principles for Electronic Banking* before 5 January 2004.

3 Reporting

Banking institutions are requested to inform the Bank of Namibia at the latest on 30 October 2003 on the following:

- Which principles have already been fully implemented;
- Which principles have been partially implemented; and,
- Implementation plans, including timeframes, for those principles that are currently not adequately addressed.

Surveys similar to the August 2003 survey will be conducted on a regular basis.

4 Additional Copies

Two additional copies of this Circular are enclosed for the use of your institution's independent auditors. The attached "Acknowledgement of Receipt" duly completed and co-signed by the said auditors, should be returned to this Office at your earliest convenience.

P. HARTMANN

DEPUTY GOVENOR