A CHECKLIST FOR YOUR

INFORMATION SECURITY PROGRAM

Each Bank must implement a "comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities".

- ❑ Establish Management Accountability (who's in charge?)
- ❑ Involve the Board of Directors (or a committee) to:
    - Oversee development, implementation and maintenance of information security program
    - Approve written information security program
    - Receive periodic reports on effectiveness of the adopted program
- ❑ Assess Risks to Customer information--Electronic and physical information
    - What information is being stored? Determine relative sensitivity
    - Where is the information stored?
    - How is it stored?
    - What are the access points to the information?
    - Who could have access?
    - Who should have access?
- ❑ Draft or revise Information Security Program based on Assessment in
- ❑ Implement Program and train all employees
- ❑ Oversee Service Providers
    - Are all contracts in writing? (July 2003, grandfather period ends)
    - Are there confidentiality/security commitments?
    - Can Bank monitor compliance with confidentiality/security commitments?
    - Has the Bank accomplished appropriate due diligence in choosing provider?
- ❑ Monitor Compliance with the Information Security Program
- ❑ Create Flexibility in the Program to respond to technology changes, threats. product development, etc.