Information Technology/Security

As most Bank's utilize a highly technical third party provider to perform IT reviews and network intrusion testing, we offer a review that serves to compliment the technical review that consists of the following areas: Acquisition of IT components and software, segregation of duties, user access management as well as remote access, information technology strategic planning, management and Board or committee review of IT functions, IT Risk Assessments, reviews for service providers and business continuity planning. We also offer the review of the Identity Theft Program as required under the FACT Act. Some sections reviews include the following:

- Network: LANS, WANS and Intranet
- Back-Up systems
- Systems Access and Controls
- Inventory Controls
- Upgrade and Patch controls
- Board and Management Oversight
- Security Testing of Systems
- Disposal of Assets
- Software Licenses and Renewals
- User Access testing
- Business Contingency Planning and Testing
- Regulatory Compliance
- Website Review
- System change authority and process
- Remote Access and Users
- Vendor Management Program and Oversight
- Virus Protection
- Social Engineering
- Mobile Devices
- Digital Signature Controls and Policies

Information Security (GLBA)

- Review of Board of Directors Oversight
- Annual Review of Program
- Evaluate the risk assessment process.
- Evaluate the adequacy of the program to manage and control risk.

Identity Theft Red Flags (FACT ACT)

- Identity Theft Program Policies and Procedures
- Evaluate the risk assessment process.
- Evaluate the adequacy of the program to manage and control risk.
- Review of testing on systems used to monitor and deter "red flags."

- Test the Bank’s address change process and monitoring efforts.