



GLBA Compliant Information Security Risk Assessment

Information security is essential for business operations and regulatory compliance. Furthermore, financial institution examiners are conducting risk focused examinations that specifically address provisions of the Gramm-Leach-Bliley Act and the FFIEC Information Technology Handbook (e.g., Information Security Booklet) which addresses the need for an enterprise-wide information security risk assessment be conducted on a yearly bases.

Heightened regulatory scrutiny is resulting in penalties and fines for non-compliance. Financial institutions must maintain an appropriate and comprehensive information security program. The program must be based on a documented risk assessment and provide for independent testing of controls. If your information security program and risk assessment do not incorporate a testing plan and comprehensively address controls over physical and digital information, you will likely fall short of the guidelines outlined in the FFIEC Information Security Booklet. A common pitfall involves an exclusive focus on technical controls (e.g., penetration testing). While these tests are an essential component, they do not fully address the baseline requirements and must be supplemented with evaluations of administrative and physical controls.

Scope of Services

NETBankAudit's Information Security Risk Assessment includes internal and external penetration testing, in addition to the evaluation of administrative and physical safeguards. The following areas are included in the scope of our comprehensive Information Security Risk Assessment:

- Internal Network Security (details provided below)
- External Network Security (details provided below)
- Information Systems Security Policies and Procedures
- Physical Security of IT Equipment and Resources
- Physical Security of Documents and Records
- Disaster Recovery and Business Continuity
- Incident Response
- Outsourcing and Vendor Management
- Information Security Testing Plan
- Management Oversight
- Employee Training and Awareness

Internal and External Network Security

The Internal and External Network Security Assessments provide comprehensive evaluations of technical controls protecting internal computer systems and the network perimeter. Our methodology involves a combination of automated vulnerability scanning tools, manual system configuration verification, and interviewing techniques.

The scope of our Internal Network Security Assessment includes the following:

- System Configuration
- Networking
- User Management
- Group Management
- Password Management
- File System Access and Management



GLBA Compliant Information Security Risk Assessment

- Sensitive System Privileges and Utilities
- Physical Access
- Remote Access
- Auditing, Logging, and Monitoring
- Security Administration Activities
- Maintenance and Operations
- Fault Tolerance, Backup and Recovery
- Modem Controls
- Desktop Assessment
- Virus Protection
- Firewall and Router Analysis
- Change Management Procedures
- Physical Security of IT Equipment and Networked Resources
- Recommendations for corrective actions to noted deficiencies

The scope of our External Network Security Assessment includes the following:

- Network reconnaissance and mapping (foot-printing).
- Vulnerability definition through the use of open source and commercial tools
- Targeted attacks using open source and commercial tools
- Open source social engineering (Google hacking, etc).
- Recommendations for corrective actions to noted deficiencies

Why NETBankAudit?

NETBankAudit was designed and developed to exclusively support the GLBA/FFIEC IT Regulatory Audit and Assessment needs of community financial institutions.

- NETBankAudit only works with community financial institutions
 - We specialize in GLBA/FFIEC audits and assessments
 - We specialize in helping our clients become and remain GLBA/FFIEC compliant
- NETBankAudit is not like our competitors
 - Accounting firms generally do not have the technical and engineering expertise needed
 - Technical firms generally do not have the regulatory and audit expertise needed
- NETBankAudit is completely independent of other products and services
 - NOTE: The **FFIEC IT Audits Booklet**, in the “**Outsourcing Internal IT Audits**” section states *"Potential conflicts of interest may arise if the outsourced auditing firm performs IT Audit functions in addition to other audit services, such as: Providing the independent financial statement, or serving in an IT or management consulting capacity."*
- NETBankAudit employees are superior:
 - Community financial institutional experience
 - Security engineering experience
 - Regulatory experience and expertise
 - All NETBankAudit engineers and auditors are full time employees (no subcontracting)
 - All NETBankAudit employees have applicable certifications (CISSP, CISA, etc.)
 - NETBankAudit performs background checks on all its employees