



Information Technology Audit

Your Financial Institution requires an information technology (IT) audit that addresses essential controls and procedures. A comprehensive IT audit is critical to identify and evaluate controls and processes for their adherence to the bank's policies. Tests of controls and processes for their effectiveness are also essential to ensure that they are achieving their stated objectives.

NETBankAudit offers a well-planned, properly structured and fully documented IT audit, which is essential to proper evaluation of risk management practices, internal control systems, and compliance with corporate policies concerning information systems related risks. A comprehensive independent IT audit is also an important requirement that is now addressed in the FFIEC's IT Audit Booklet and will also encompass the guidance outlined in the FFIEC's twelve information systems booklets, in addition to other recent regulatory guidance (e.g., OCC, FDIC, Federal Reserve, OTS, and NCUA publications and guidance addressing IT control considerations). IT Audit is also an important component of a company's Sarbanes-Oxley Act (SOX) compliance. To address these requirements, NETBankAudit follows an approach and methodology that is based on existing FFIEC regulatory guidance and recognized industry standards (e.g., CoBIT). Our process evaluates the institution's information systems environment, including technical, administrative, and physical controls by testing and documenting their effectiveness. The audit is documented in a detailed report and supporting work-papers that provide a helpful resource for management and examiners.

Specific areas that will be covered by the audit will include the following:

Information Technology Management

- Board and Senior Management Oversight
- Job Descriptions and Organizational Structure
- Strategic Planning and Project Management
- Risk Assessment Process
- Regulatory Compliance (Information Security Program)
- Testing and Audit Provisions
- Training and Awareness
- Outsourcing and Vendor Management
- Insurance Coverage

Information Technology Operations

- Information Systems Policies and Procedures
- Data Integrity and Input/Output Controls
- Network Administration and Documentation
- User-Related Controls
- Software and Application Controls
- Hardware and Computer Equipment Controls
- System Maintenance and Change Management
- Data Backup
- Business Continuity and Disaster Recovery

Information Technology Security

- Network Architecture and Security
- Logical and Administrative Access



Information Technology Audit

- Logging, Monitoring, and Data Collection
- Physical Security Controls
- Incident Response

Payment Systems and Electronic Banking

- Internet Banking
- Telephone Banking
- ATMs and Debit Cards
- Wire Transfer and ACH

NETBankAudit's comprehensive IT Audit includes internal and external network testing. The scope of the testing includes the following:

Internal Network Security Assessment (Includes but not limited to)

- System Configuration
- Networking
- User Management
- Group Management
- Password Management
- File System Access and Management
- 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
- Application Security
- Windows Diagnostic Review
- Desktop Assessment
- Virus Protection
- Firewall and Router Analysis
- Change Management Procedures
- Physical Security of IT Equipment and Networked Resources
- Internal Network Scanning for Known Vulnerabilities
- Information Security Program (Policy and Procedure) Review
- Information Security Risk Assessment (GLBA) Review

External Network Security Assessment

- Passive electronic discovery of identified targets
- Active discovery of the target networks/domains
- ICMP and UDP style trace-routes, in addition to Ping Sweeps, to map the network and identify routes, active hosts, firewalls, etc.
- Reconnaissance and target research, including intense scans on identified and branded hosts
- Bulk vulnerability scanning



Information Technology Audit

- Manual verification of the discovered vulnerabilities to confirm that they are not "false positives"
- Applicable application attacks, including brute force attacks, CGI exploits, and Web server assaults

To ensure the appropriateness of the audit, NETBankAudit will work closely with you to plan for a scope that is tailored for your bank and its IT risk profile.

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 Audit 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