



## IT Vulnerability Assessment

---

In today's environment, your financial institution's computer network is essential to business operations. This becomes painfully evident when system downtime prevents employees from completing their daily work and communicating with financial institution's customers. Furthermore, networked resources, which include systems containing confidential customer data, are vulnerable to unauthorized access and damage from internal and external threats. The only way to ensure that your networked environment is appropriately safeguarded is to implement security controls and test them regularly. Recognizing the importance of network security, financial institution regulators are requiring that independent security assessments are performed at least annually. If your IT environment has not been comprehensively tested, you may fail to meet the guidelines outlined in the *FFIEC Information Security Booklet*.

### Scope of Services

Our 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 internal and external assessments can be conducted separately or in combination.

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
- 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
- Information Systems Security Policies and Procedures
- Disaster Recovery and Business Continuity
- Incident Response
- Outsourcing and Vendor Management
- Recommendations for corrective actions to noted deficiencies

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



## IT Vulnerability Assessment

---

- Network reconnaissance and mapping (footprinting).
- 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 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