Financial Institution Compliance: IT Audit

Weaver's experienced IT audit team provides financial institutions with a thorough analysis of weaknesses in the system that might provide access points for internal or external data breaches. An IT audit evaluates your financial institution's computer systems for potential vulnerabilities to external threats and internal compromise. In order to best safeguard the integrity of you and your customers' data, an IT audit evaluates the controls within your infrastructure to protect your institution from a wide range of internal and external security threats.

A variety of state, federal and international regulations require independent verification of IT systems and controls, including:

- Federal Financial Institutions Examination Council (FFIEC)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Federal Deposit Insurance Corporation Improvement Act (FDICIA)

IT Controls Evaluations

An IT audit can identify weaknesses in your existing infrastructure, highlighting areas of concern and potential liabilities for a financial institution. By evaluating your system before a breach occurs, an IT audit can significantly mitigate financial loss from fraud or theft, productivity loss from system downtime, and the risk of compromising customer data and proprietary operating information.

Weaver's IT audits review the following objectives: wholesale payment systems, e-banking, outsourcing technology services, business continuity planning, information security, retail payment systems, development and acquisition, supervision of technology service providers and operations and management.

Systems We Know:

- BankTEL
- Callidus
- Cardinal
- Dynamics SL
- FedLine
- FEDLINK
- FIS HORIZON
- Fiserv
- Great Plains / Microsoft Dynamics GP
- Jack Henry CIF 20/20
- Jack Henry Silverlake
- Pershing
- Q2
- Salesforce
- SEI
- SRG WLS

weaver
Assurance • Tax • Advisory

Security Services

Cybersecurity concerns are at an all-time high. Identifying vulnerabilities is the first step toward protecting the confidentiality, integrity and availability of critical data. Weaver offers a range of security services and the following are highlighted services that are required by the FFIEC IT Examination Handbooks and help management evaluate security risk.

Network Perimeter Security:

The FFIEC IT Examination Handbooks call for management to periodically undergo independent assessments of network security. We propose to conduct our network security procedures in two phases:

Network Vulnerability Scanning is our automated scanning technology that helps management identify and manage vulnerabilities in systems attached to the bank's network. Our teams provide value by interpreting results from the scan and providing management with clear recommendations. We work with management to obtain responses that are incorporated into the final report.

External Network Penetration Testing includes manual and/or automated procedures that are designed to test whether an unauthorized external user can gain access to the bank's internal IT resources or create an issue with availability.

Social Engineering:

Bank staff can serve as either a key line of defense or an unlocked back door. Using social engineering techniques, Weaver staff can test for human vulnerabilities such as staff who will share a password or who will click a link in a suspicious email. Social engineering activities include:

A public information search, examining publicly discoverable information to identify potential vulnerabilities through disclosure of sensitive data.

Email phishing and phone call phishing (vishing), in which Weaver will attempt to lure bank employees into disclosing inappropriate information or opening a potentially exploitable back door into a bank system.

Additional procedures are available such as physical media baiting (i.e. USB drives) and physical access testing (i.e. tailgating).

For more information contact:

Brian Thomas, CISA, CISSP, QSA
Partner, IT Advisory Services
brian.thomas@weaver.com
713.800.1050

Neha Patel, CPA, CISA
Partner, IT Advisory Services
neha.patel@weaver.com
972.448.9804

Brittany George, CISA, QSA
Senior Manager, IT Advisory Services
brittany.george@weaver.com
972.448.9299