Information Technology (IT) Audit Services

infotex conducts various assessments to assist you in following your IT Audit Program. Not only does our process address the non-technical aspects of your business, but also technical aspects. Our certified Auditors and Security Analysts provide a comprehensive approach to your IT Audit Program.

GLBA Risk Assessment

This assessment will identify, measure, and manage risk arising from information. A filtering process will be created to notify business process owners of relevant risk and controls in other business processes, resulting in a reduction of redundant mitigating controls, and an alignment of information security practices with IT Governance and overall Business Strategy.

IT Governance Review (General IT Controls)

infotex will review your IT management practices, the process of which will assess the IT controls related to processes, policies, procedures, and training. **infotex** will also perform a risk assessment relating to policies and procedures, human threats, vendor threats, and other FFIEC compliance related threats.

Internet Banking Controls Review

infotex will perform an IT security review of your Internet banking controls. The review will address the most recent guidances on Internet banking issued by regulators.

Physical Security and Environmental Controls Review

We will review your physical security and environmental controls of key security zones, including, but not limited to your headquarters facility, Data Center, and branch offices. **infotex** will also review your procedures regarding physical security and environmental controls in accordance with regulatory requirements.

Business Continuity Plan and Failover Testing

We help your Business Continuity Team implement walk-throughs, table-top tests, or full functional testing. **infotex** will help design the test objectives and the test plan, and document the results as well as the post-mortem analysis all within FFIEC guidelines.

Technical Controls Review

- *External/Blind Scan (Penetration Testing)* - **infotex** will utilize the latest "attack methods" to attempt to access your internal network from outside your network perimeter.
- *Internal Network Scan* - Upon completion of the external scan, we install a proprietary device on your network that will establish a VPN to our Network Operations Center and scan for security vulnerabilities.
- *Password File Analysis* – **infotex** performs this analysis to demonstrate the importance of strong passwords as well as measure the enforcement of your existing password policy.
- *Social Engineering Tests* – In an attempt to test user-level awareness, we perform various "social engineering" services in an attempt to test user-level awareness. Social engineering tests include:
    - Spear Phishing
    - Physical Breach Testing
    - Pretext Calling
    - Ask us about our other tests!

Network Configuration Audit

infotex will perform an assessment of your current network configuration including client and server applications and IT practices based on comparison to vendor and industry published best practices. We use Microsoft Baseline Security Analyzer for Microsoft devices and review vendor documentation for AVS, Spyware Defense, Firewalls, etc.

Application Security Audits

infotex has "coders," and can perform Application Security Audits or Reviews using a phased approach. Yes, we look at the source code. And not only do we look at technical controls, but also non-technical controls (SDLC, Change Management, Documentation) that your organization has in place. We test control processes, user interfaces, encryption, authentication, infrastructure, and of course we perform extensive source code reviews. We can conduct a full audit, black-box review, or a risk-based audit (using OWASP's Top 10 as a framework).

> *"An untested control is not a control, it is a wish."*