Our audit process addresses the non-technical, technical, and people aspects of your business, allowing our certified (CISA, CISSP) auditors and security analysts to provide a comprehensive approach to your IT Audit Program. Beginning with an audit risk assessment, we ensure your audits provide the most value.

Non-Technical Tests

Audit Risk Assessment

Our audits always start with a risk assessment meant to identify key controls . . . why test controls that mitigate no risk at the expense of testing controls that mitigate the most risk? This becomes the basis of our audit plan.

IT Governance | General IT Controls

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

Asset Specific (i.e. Internet Banking) Controls Review

From mobile security to mobile banking, we perform an IT security review of controls declared for specific assets which your audit risk assessment warrants testing. These reviews will cover best practices, but also address the most recent guidance issued by regulators.

Physical Security and Environmental Controls Review

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

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:

- Pretext Calling
- Phishing, Vishing, and Spear Phishing
- Phone Phishing
- Physical Breach Attempts
- Dumpster Diving, Clean Desktop Walkthroughs, Trashcan Reviews

Ongoing Pretext Calls

In this service, we perform pretext calls all year long, so that you can tell users that every time they answer the phone, it could be a test.

Password File Analysis

We perform this analysis to demonstrate the importance of strong passwords as well as measure the enforcement of your existing password policy.

Public Presence Reviews

We can analyze what others can find on your bank and its employees "in the public presence." Like a social engineering test, a public presence review can act as a preventive control.

Social Media Reviews

To help you understand what's being said, how and where, we will usually target three groups: your customers, your employees, your managers.

Penetration Tests

We can target your "system" mimicking technical and nontechnical attack methods in a "capture-the-flag" exercise. Whether for PCI compliance, Incident Response functional testing, or technical awareness, we find that the penetration test, especially one that lasts 10-14 months, is the best way to activate awareness.

Technical Tests

External Blind Scan

We 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.

Network Configuration Audit

We perform an assessment of your current network configuration in accordance with vendor and industry best practices using Microsoft Baseline Security Analyzer. This includes all client and server applications as well as IT practices. We review vendor documentation for AVS, spyware defense, firewalls, and more.

Web Application Security Review

Our Web Application Security Review is performed using a phased approach. We look at both technical and non-technical controls active within your organization. These controls include but are not limited to SDLC, Change Management, and Documentation. We test control processes, user interfaces, encryption, authentication, infrastructure, and 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).

Virtual Environment Review

We review the configuration of your virtual environment using SANS Institute publications and vendor publications as a best practice framework. This review takes into consideration visibility, configuration management, network management, and disaster recovery as well as security.

Email Configuration Audit

How do you know your e-mail is configured with best practices in mind? What if secure messages do are not configured securely? Are vulnerabilities properly addressed? These include not only technical vulnerabilities, like anti-malware and secure messaging configurations, but also the way e-mail aliases are set up. With this audit, we provide third party assurance to management so that there is never any question, and so that you don't end up with a false sense of security.

Printer Vulnerability Assessment

All copiers and multifunction devices, and most printers, have memory even if it's just onboard flash memory. This includes all multifunction devices.

This assessment implements new audit controls to eliminate the impact of "intrusive scanning." We then scan network connected printers and multifunction devices for vulnerabilities and common misconfiguration issues. The resulting risk mitigation makes it an audit test worth considering!

Other Assessments

Network Support Provider Risk Review

This review produces a report very similar in format to the SOC2 Report about the existing and veracity of declared controls.

Tabletop Testing

We help your Incident Response and/or Business Continuity Team implement walk-throughs, table-top tests, and/or or full functional testing. From the test plan to the post-mortem analysis, we put your management team on the same page as your contingency planning, all within FFIEC guidelines.