

Auditing IT: Identifying Exposures in Your Environment

Course Duration: 1 Day
CPE Hours: 8 Hours
Level: Intermediate/Group-Live
Prerequisites: None
Advanced Preparation: None

Recent newspaper stories concerning identify theft and vital records exposure are causing concerns in boardrooms across the country. How could these things happen at SOX-compliant companies? The answer is that the SOX effort focused primarily on applications and transactions. Testing at the operating system and database level focused primarily on general controls. This seminar is intended for auditors who now want to make the extra effort to ensure that the systems and databases hosting SOX-compliant applications are secure. Using the Canaudit audit approach, security is analyzed using a combination of scripts, tools and yes, even exploits, to identify weaknesses before they can be exploited by hackers.

Who Should Attend:

This seminar is intended for IT auditors, integrated auditors and audit management.

Seminar Outline:

I) Understanding the Environment

- Identifying the information risks in your network
- The general controls review
- Physical security
- Social engineering
- The network scan
- The initial testing and risk assessment
- Determining the IT risk universe
- Scoping the audits

II) The Perimeter Audit

- Identifying external connections to the network
 - ⇒ Dial in and out
 - ⇒ Wireless
 - ⇒ Internet
 - ⇒ Inside-out, outside-in issues
- Firewalls, IPS and IDS
- VPNs, model pools, etc.

III) The Network Audit

- Securing and segmenting the network
- Network device and appliance security
- Monitoring network activity

- Monitoring connectivity and pattern changes
- Incident response procedures and techniques

IV) The Windows Audit

- Identifying poorly secured machines
- Determining patch levels
- Passwords, the Achilles' heel of Windows
- Vulnerability testing
- Security implementation, local and server
- Audit implementation, local and server
- Two factor authentication
- Administration and maintenance

V) The UNIX Audit

- Using services to take control of a system
- Known exploits
- Trust relationships
- File insecurity
- Patch and change management

VI) The Mainframe Audit

- So you have RACF
- Securing critical libraries and files
- Critical attack areas and prevention techniques

- Proactive security versus reactive security
- Cross environment exposures

VII) The Database Audit

- Excessive rights
- Backdoor accounts and default password
- Poorly secured exports and backups
- Role proliferation
- Remote access
- Operation and maintenance

VIII) The Penetration Audit

- The ultimate test of preparedness
- Internet and e-business exposures
- Rogue wireless access points
- Undocumented dial-in access
- Trading partner connections
- The internal test
- Vulnerability assessment and conclusion

IX) Closing Comments