

# Hands-On: Performing an IT Audit and Security Baseline

<b>Course Duration:</b>	4 Days
<b>CPE Hours:</b>	32 Hours
<b>Level:</b>	Beginner to Intermediate/Group-Live
<b>Prerequisites:</b>	None
<b>Advanced Preparation:</b>	None

Every week, several major organizations are reporting data breaches. Despite the time and effort completing Sarbanes-Oxley or HIPAA reviews, overall security has not improved. The IT Audit and Security functions are inundated with regulatory testing to the point where they are unable to complete the required IT Audit or Security regimens. This includes projects to ensure that the controls are in place to protect confidential information and to prevent identity theft or the compromise of sensitive financial data. This 4-day, hands-on workshop will teach attendees the skills needed to perform an IT Audit and Security Baseline. Participants will learn how to identify poorly secured operating systems, databases and wireless, dial-up and Internet vulnerabilities. Over the course of the 4 days, the participants will complete a series of simulations and exercises designed to build the knowledge to safely and sanely use available tools. These tools identify critical security issues in the enterprise-wide network. To assist in the transfer of skills, the workshop instructors are available post-seminar to provide assistance. Participants are required to have a network-enabled Win2K/XP/Vista laptop with administrative rights to both the operating system and anti-virus software (to create a directory exempt from anti-virus scanning), an office suite with word processing and spreadsheet capabilities (i.e. MS Word and Excel), and a CD-ROM drive.

## Who Should Attend:

This class is intended for new IT auditors, financial or integrated auditors making the transition to IT auditing, and existing IT auditors who need to refresh their skills.

## Seminar Outline:

- I Overview**
  - Why conduct an IT Audit or Security Review
  - The Canaudit Methodology
  - Skill sets required
  - Tools and techniques
  - Anticipating the hurdles
  - Preparing project plan
  - Schedule testing
  - Communicating project to IT group
  - Getting started
- II Network Devices**
  - Security risks associated with the network and network devices
  - Preparing for the network review
  - Identifying network segments
  - Installing network tools
  - Configuring parameters
  - Starting scans
  - Monitoring the process
  - Analyzing results related to network devices
- III Documenting the Network and the Devices Within It**
  - Using network scans to document network
  - Categorizing devices (Windows, UNIX, Linux, AS/400, Mainframe, databases)
  - Building master spreadsheet
  - Risk assessment by machine category
  - Identifying vulnerable systems
  - Safe and sane testing techniques
  - Documentation and reporting
- IV UNIX and Linux Testing**
  - Scan results and service analysis
  - Using finger, VRFY and EXPN to identify accounts
  - Testing for default passwords
  - Identifying and testing trust relationships
  - Patch testing
- V Windows Environment**
  - Scan results and vulnerability assessment
  - Tools and techniques to safely test
  - Testing for critical flaws
  - Leveraging flaws to enhance access
  - Accessing critical applications
  - Workpapers reporting and remediation plans
- VI Mainframe and I Series (AS/400)**
  - Reviewing scan results to identify mainframe and other major IBM platforms
  - Using poorly secured services to bypass access control software
  - Gaining enhanced rights using cross-over accounts
  - Proving read and write access to critical libraries
  - Reporting and documenting the issues
- VII Database Assessment**
  - Scanning to identify poorly secured databases
  - Gaining enhanced access to Oracle
  - Gaining access to MS SQL and MySQL
  - Gaining access to Sybase and Informix
- VIII Wireless**
  - Preparing for wireless test
  - Wireless software configuration
  - Identification of in-scope wireless access points
  - Evaluating encryption and other security mechanisms
  - Testing resiliency of wireless network
- IX Dial-up**
  - Selecting tools for dial-up test
  - Identification of phone ranges and scope limitation
  - Identification of responding dial-up devices
  - Vulnerability assessment of each entry point
  - Items missed by normal dial testing
  - Need for manual inspection of some devices
  - Quantifying the exposure
- X The Internet**
  - Accessing skills level of project staff
  - Test in-house or co-source
  - Identifying Internet footprint
  - Scanning and mapping the Internet presence
  - Testing tools and techniques
  - Understanding the risk and testing for web vulnerabilities such as cross-site scripting and SQL injection
- XI Evaluating and Reporting**
  - Preparing report sections
  - Developing realistic solutions
  - Segmenting no-cost/low-cost items for remediation
  - Identification of high-cost, longer-term solutions
  - Preparing project closing conference
  - Preparation of report
  - Scheduling remediation testing
- XII Help is Available**
  - What you have learned
  - The daunting task ahead
  - Getting management to buy in
  - Planning and budgeting
  - Identifying skills deficiencies
  - Selecting resources to fill skills gaps
  - The co-sourcing option