

IT Audit and Security Boot Camp

Course Duration:	5 Days
CPE Hours:	40 Hours
Level:	Intermediate/Group-Live
Prerequisites:	None
Advanced Preparation:	None

This intensive training session combines over ten days of training and fourteen hundred pages of material into a one-week technical audit boot camp. Under the skillful guidance of Canaudit's best instructors, participants will learn how to perform complex technical audits using the Canaudit Audit Approach. The Boot Camp starts with a session on IT Audit Risk and preparation of an effective IT Audit Plan. Next, participants are prepared to audit the most common areas in IT. This approach provides the knowledge needed for participants to conduct a series of rapid-fire technical audits when they return to the office. Over a three to six month period, a General Controls Review, Network Audit, several Operating System Audits and a review of the Internet should be able to be completed. Using the Canaudit Technical Audit Guides, which are COSO compliant, field times are reduced for each audit while increasing audit scope and depth of coverage. Participants will also learn how to effectively report issues to management, while providing the IT administrators and technicians with a working document allowing them to correct existing security issues. The administrators and technicians will then be able to build a strong control structure to ensure that future weaknesses are detected and corrected. Due to the intensity of this class, homework is assigned every day. 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 Boot Camp 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) The IT Risk Assessment

- IT Risk universe
- Historical risk models
- Understanding new IT risks
- The Canaudit Technical Risk Assessment
- Creating the IT Audit Plan
- Timing and budgets
- Presenting the plan to management

II) A New Approach to General Controls

- Physical security post 9/11
- Logical security in a hacker-infested world
- Business continuance: Surviving and thriving when others fail
- Disaster preparedness: When all else fails, planning prevails
- Storage management: Protecting your assets
- Evaluating IT organizational effectiveness
- Risk/Control tables
- The Canaudit General Controls Audit Guide

III) Network Control and Security

- Auditing the carriers
- Understanding and auditing communication alternatives
- Auditing network equipment and configuration

- Auditing the wire-based intranet
- Auditing dial-up access
- Auditing wireless networks
- Auditing VPN connections
- Mapping the network
- Trading partner connectivity
- Network management and operations
- Risk/Control tables
- The Canaudit Network Audit Guide

IV) Control and Security of UNIX

- Understanding UNIX
- System Command Directories
- Filesystems
- The Superuser
- UNIX communications
- UNIX security
- Using the Canaudit Audit Scripts
- Risk/Control tables
- The Canaudit UNIX Audit Guide

V) Auditing Windows

- Understanding Windows
- Understanding Active Directory
- File system administration
- User and group administration
- Overall security
 - ⇒ Differences between Windows versions
 - ⇒ Policies
 - ⇒ Logs

- Risk/Control tables
- The Canaudit Windows Audit Guide

VI) Internet Control and Security

- Internet security basics
- Internet communications and architecture
- Securing the web presence
- Controlling Internet connections
- Understanding and responding to attacks
- Tools and techniques of the hacking trade
- Vulnerabilities and exploits
- Building and maintaining secure firewalls
- Hardening your network
- Risk/Control tables
- The Canaudit Internet Audit Guide

VII) Putting It All Together

- Auditing for security and impact
- Staging the audits
- Presenting issues in an understandable format
- Writing audit reports
- Follow-up: Tracking control implementation
- What comes next
- Closing comments