

Control & Security of Telecommunication Networks

COURSE DURATION: 2-days

CPE HOURS: 16

LEVEL: Intermediate / Group-Live

PREREQUISITES: None

ADVANCE PREPARATION: None

The Internet, wireless networks, VPN connections, Voice over IP and mobile computing has dramatically changed corporate networks. New threats, such as electronic espionage, cyber terrorism and the normal hacker require preemptive security and effective response countermeasures. This seminar will provide the participants with a sound grounding in modern telecommunications methodologies, performance issues and security. The instructor will demonstrate many of the automated tools required to perform a network audit or security assessment. In addition, each participant will receive the Canaudit Network Audit Guide to enable them to perform a full network review. After this session, the participants will be able to identify potential points of penetration and ensure that the business-computing environment is protected.

This seminar addresses the total network! You will learn about network components and their specific risks, along with control techniques needed to provide a safe processing environment. Handouts include control checklists to help participants identify potential threats and develop a comprehensive risk assessment.

WHO SHOULD ATTEND

This seminar is intended for IT auditors, security officers, network administrators & information systems professionals.

SEMINAR OUTLINE

I Understanding Networks

- Evolution of modern networks
- E-business technology
- Wireless connectivity
- Internet and VPN
- Remote VS local access
- Glossary of terminology

II Carrier Related Issues

- Multiple carrier environments
- Selecting required services
- Cost effectiveness
- Business continuance and disaster preparedness
- Network contracts
- Control checklist/ audit program

III Communications Alternatives

- "Wire Line" type circuits
- Broadcast type circuits
- Wireless
 - 802.11A&B
 - Bluetooth
- Voice over IP
- ISDN, B-ISDN
- Frame Relay, ATM & Cell Relay
- Identifying potential points of failure
- Risk/control summaries
- Control checklist/ audit program

IV The Internet

- Internet security

- Measures & countermeasures
- Ports, services & protocols
- Firewall configuration
- Bypassing the firewall
- Managing the firewall
- Monitoring Internet activity
- Intrusion detection & response
- Risk/control summaries
- Control checklist/ audit program

V Network Equipment and Configuration

- Routers
- Hubs
- Switches
- Wireless AP's
- Internal firewalls
- Intrusion detection & response
- Risk/control summaries
- Control checklist/ audit program

VI Mapping the Network

- Scanners
- Sniffers
- Mapping tools
- Segment mapping
- Server identification & analysis
- Undocumented connectivity
- Security & connectivity contracts
- Identifying vulnerabilities
- Risk/Control Summaries
- Control checklist/ audit program

VII Trading Partner Connectivity

- Identifying trading partner connections
- Trading partner servers within the network
- Title VS connectivity
- Enforcing security arrangements
- Risk/control summaries
- Control checklist/ audit program

VIII Network Operations and Management

- Business continuance and disaster preparedness
- Maintenance/Problem reporting
- Load management
- Network monitors
- Network utilization & trend analysis
- Management & exception reporting
- /control summaries
- Control checklist/ audit program

IX Network Incident Management

- Network Incident response procedure
- The network response team
- Investigating/ prosecuting intruders