



IT AUDIT AND SECURITY SEMINARS

2010 COURSE CATALOG

SecureIT

1902 Campus Commons Drive, Suite 100

Reston, VA 20191

Phone: (703) 464-7010

Fax: (703) 464-5990

Email: training@secureit.com

Website: www.secureit.com

SECUREIT CORPORATE OVERVIEW

SecureIT's core competency is our industry-leading security, compliance, and audit expertise. Our intellectual capital, processes and relationships build on our professional talent and position us to serve clients as trusted, competency-focused advisers.

The technical qualifications, expertise and talent of our professionals are the foundation of our capabilities. SecureIT integrates technical and business expertise in creating effective security solutions that span technology, people and processes. Our four main service offerings are outlined below:

Enterprise Security

Finding and Remediating Vulnerabilities

SecureIT offers a comprehensive range of services to help clients assess their threats, vulnerabilities, and risks; design and implement information security strategies and programs; and improve their information assurance capabilities through monitoring, periodic reviews, and audits. Our information security services are based on a risk-based methodology for protecting the confidentiality, integrity, and availability of information. In addition, we strongly recommend that our clients pursue a holistic approach to information security. To support this approach, we tailor solutions to our clients' specific needs, or facilitate transformation of their information security function and capabilities. Enterprise Security service offerings include:

- CISO Advisory
- Application Security & Controls Assessment
- Security Strategy & Governance
- Security Policy and Procedure Development
- Security Architecture
- Security Program Implementation
- Secure Application Architecture & Design
- Business Continuity and Contingency Planning
- Penetration Testing & Vulnerability Assessment
- Security Baseline Configuration Management & Compliance
- Database Security Monitoring
- Computer Forensics & Incident Response

Governance, Risk & Compliance (GRC)

Minimizing Risk, Maximizing Value

SecureIT's governance, risk and compliance services focus on identifying and mitigating the risks inherent in using information systems to support business objectives. We combine technology best practices expertise, industry knowledge and managerial experiences to help clients manage their technology risks and maximize return on their IT investments, all the while complying with applicable laws and regulations. GRC related service offerings include:

- Enterprise Risk Assessment
- Regulatory Compliance
- Controls Framework Implementations and Assessments
- Audit Readiness & Liaison
- PCI Qualified Security Assessor
- SAS70 Reviews & Readiness Assessments
- Privacy Risk Management
- Vendor Risk Management
- Merger & Acquisition IT Controls Diligence

IT Audit

Helping You Run a Tighter Ship

Organizations today face a variety of demands for internal audits — including new laws and regulations, competitive pressure and technological change. SecureIT's specialists rely on deep technical skills and industry knowledge to develop or improve internal audit functions with quality, efficiency and effectiveness. Our services include instituting risk-based IT audit strategies; performing IT audit projects; and providing ongoing expertise through co-sourcing arrangements.

Our methodology can produce significant, measurable impacts on the cost effectiveness of the IT audit function and its value to our clients' internal control and corporate governance. IT Audit service offerings include:

- IT Audit Strategy & Planning
- IT Audit Co-sourcing/Outsourcing
- Deep-dive Infrastructure and Application Security Audits
- IT Audit Training
- Data Mining & Analysis
- IT Audit Quality Assurance Review

Training

The Knowledge and Tools for Success

SecureIT offers numerous seminars throughout the year, and we deliver custom training programs to our clients. Our goal is to provide high quality and practical training to IT audit and information security professionals. SecureIT's training solutions are a vehicle for sharing our intellectual capital with our clients and professional communities. Our course offerings are information-packed, assurance-focused and modular, and SecureIT provides supplementary information and tools to enhance the quality of our training solutions.

SECUREIT CLIENTS

We are proud of the fact that many top-tier organizations have engaged SecureIT and depend on us for their Security, Information Assurance, Governance, Compliance, and IT Audit needs. Our clients include Federal agencies, leading commercial organizations, and nonprofit entities. More significantly, our diverse client mix provides us with opportunities to develop cross-industry best practices based on a deep understanding of our clients' business models.

SecureIT's notable clients include:

Commercial Clients

Allied World Assurance
 Beers & Cutler
 Constellation Energy
 CSC
 E*Trade Financial
 Ernst & Young
 FINRA
 Freddie Mac
 HMS Host
 InterAmerican Development Bank
 International Monetary Fund
 ICMA
 Karmanos Cancer Institute
 McKesson Corporation
 Promontory Financial
 Tier Technologies
 The Washington Post
 Watson Wyatt
 Westat

Government Clients

Centers for Medicare and Medicaid (CMS)
 Defense Information Systems Agency (DISA)
 Department of Commerce (DOC)
 Department of Education (DOED)
 Department of Health & Human Services (HHS)
 Department of Justice (DOJ)
 Department of Labor (DOL)
 Department of Treasury
 Department of Veterans Affairs (VA)
 Export-Import Bank (EXIM)
 Federal Aviation Administration (FAA)
 Federal Trade Commission (FTC)
 National Aeronautics and Space Administration (NASA)
 United States Agency for International Development (USAID)
 United States Marshalls Service
 United States Postal Service (USPS)

SECUREIT TRAINING SERVICES

SecureIT conducts numerous IT Audit and Information Security training seminars throughout the year. Our goal is to provide quality, **practical** training to the IT Audit community. As such, there are several things that set us apart from other IT Audit training providers:

- Information-packed sessions: We've cut the "fluff" from our presentations so that the maximum amount of material can be covered in a minimal amount of time.
- Technical approach: The technical material that we present is covered in detail, especially for network and platform technologies. Our courses start at an introductory level, but address intermediate and advanced topics as needed.
- Detailed slides: SecureIT develops content-packed slides (as opposed to high-level bullets) that can be used as a reference at a later point in time or for research during an actual audit/review.
- Audit-focused: All topics (even technical security issues) are covered from an auditor's perspective. Most of our modules have listings of key controls and key audit procedures which can be used to construct an audit program or security review approach.
- Highly modularized courses: SecureIT has developed each training in a modularized fashion. As such, we are able to customize each of our trainings by adding, deleting, or switching modules to address the unique training needs of our clients.

In addition to sponsoring public training seminars throughout the year, SecureIT has delivered IT audit and security trainings for multiple IIA, ISSA, and ISACA Chapters (including Washington DC, New York, Minneapolis, Baltimore, Dallas, Philadelphia, Hartford, Boston, Tampa, Middle Tennessee, Sacramento and Chicago), as well as at organizations such as Freddie Mac, US Government Accountability Office (GAO), Cotton and Company, State of Virginia, Johns Hopkins, US Postal Service OIG, and the MIS Training Institute.

SEMINAR LISTING

The following are SecureIT's current IT audit and security seminar offerings. However, please check our website (<http://www.secureit.com>) for our up-to-date listings, as we make frequent changes to the catalog.

- [IT Audit Bootcamp](#) (2 days)
- [Advanced IT Auditing](#) (3 days)
- [Auditing Cisco Routers](#) (2 days)
- [Auditing Checkpoint Firewalls](#) (2 days)
- [Intrusion Detection Systems & Intrusion Response](#) (1 day)
- [Network Security Bootcamp for IT Auditors](#) (5 days)
- [Auditing Solaris](#) (2 days)
- [Auditing Microsoft IIS 6.0](#) (1 day)
- [Auditing Windows 2003 Servers and Domains](#) (3 days)
- [Auditing Oracle Databases Security](#) (2 days)
- [Auditing Web Server and Web Application Security](#) (2 days)
- [Auditing Wireless Security](#) (2 days)
- [Entity-Wide Security Management](#) (2 days)
- [Security Essentials: Intro to the CISSP Common Body of Knowledge](#) (1 day)
- [Introduction to Encryption and PKI](#) (1 day)
- [Using ACL for Data Analysis](#) (1 day)
- [CISSP Boot Camp](#) (5 days)
- [Ethical Hacking](#) (5 days)
- [Computer Forensics Training](#) (5 days)

IT AUDIT BOOTCAMP

Overview:

This seminar will give participants the knowledge necessary to understand and effectively evaluate controls in an information processing environment. It will outline and define basic technical concepts, and provide a risk-based approach for ensuring that adequate controls have been implemented. The seminar will incorporate guidance contained in leading industry standards, most notably the Control Objectives for Information Technology (COBIT), the Federal Information Systems Controls Audit Manual (FISCAM), and ISO 17799. It will begin at a very basic level and slowly progress into more complex technology issues that are prevalent in today's information processing environments. The seminar will consist of modules that address the core areas of IT risk. Each module will explain the objectives, risks, key controls, and primary audit procedures that can be used. You will leave this seminar with a solid knowledge of key technology concepts, and the foundation needed to audit these technologies and processes effectively.

Audience:

This seminar is designed for entry-level IT Auditors, and financial auditors interested in making the move to IT.

Prerequisites:

None

Outline:

- Information Technology Risk
- Categories of Risks and Controls
- IT Control Environment
- Security Management
- Systems Management
- Systems Development
- Change Management
- Network Security
- Auditing Operating System Security
- Physical, Environmental, & Operations Management
- Disaster Recovery & Business Continuity
- Database Management
- Data Management
- Introduction to Application Controls
- Types of Audits

Seminar Duration:

2 days (15 CPEs)

[Return to Seminar Listing](#)

ADVANCED IT AUDITING

Overview:

This seminar, designed specifically for government and private-sector IT Auditors, will provide the tools and techniques needed to effectively understand and audit modern distributed and web-based applications. The control techniques that are used to address risk in distributed and web-based systems are substantially different from the traditional techniques used in legacy mainframe environments. Unlike many generic Application Auditing seminars, this seminar will focus specifically on distributed system control techniques and the unique risks of the supporting technologies. This seminar addresses infrastructure controls (network security, electronic communications, etc.) as well as application and middleware controls (transactional integrity, application recoverability, etc.) that protect the reliability and integrity of critical data. Every module of this seminar will outline “best practice” control techniques and include suggested audit procedures. The seminar incorporates standard auditing control objectives such as GAO’s FISCAM, ISACA’s COBIT, and ISACF’s Objectives for NetCentric Technology. The lectures and seminar materials will complement these established guidelines by providing practical steps for performing effective audits of modern network-based and web applications.

Audience:

IT Audit professionals, and others tasked with evaluating controls over modern distributed and web-based applications.

Prerequisites:

None

Outline:

- Information Technology Risk
- Auditing Security Management
- Auditing Systems Management
- Auditing Change Management
- Auditing Network Security
- Auditing Platform Operating System Security
- Auditing Database Management
- Auditing Data Management
- Auditing Electronic Communications
- Auditing Encryption & VPNs
- Auditing Application Controls
- Application Security Architectures
- Auditing Application Security Management
- Auditing Data Accuracy and Validation
- Auditing Input / Output Controls
- Auditing Balancing and File Version Controls
- Auditing Transactional Integrity
- Auditing Application Recoverability
- Auditing Web-based Applications
- Auditing OO and Java Applications

Seminar Duration:

3 days (22 CPEs)

AUDITING CISCO ROUTERS

Overview:

This technical seminar will give participants the knowledge necessary to thoroughly understand and effectively evaluate the configuration of a Cisco router. This industry-leading router will be discussed in depth and hands-on case studies will reinforce important concepts learned. With increased connectivity to the Internet, organizations can no longer simply rely on operating system security to protect their valuable corporate data. They must also rely on other network security components to provide this protection, including firewalls, intrusion detection systems, and routers. These components must be properly configured to ensure that only authorized network traffic is able to pass through to internal networks. This course will help participants understand the various components of a Cisco router and give them the tools needed to effectively audit their configurations.

Audience:

This seminar is targeted towards mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies. Prior exposure to routers will be useful but is not required.

Outline:

- Introduction to Routers
- Routers & Network Security
- TCP/IP Internetworking
- Network Interfaces & Routes
- Basic Access Lists
- Advanced Access Lists
- Hardening Router IOS & Services
- Terminal Line Authentication & Access Controls
- Security Servers & Cisco AAA
- Router Advanced Features
- Change & Systems Management
- Logging & Monitoring
- Approach for Auditing Cisco Routers
- Cisco Router Case Study

Seminar Duration:

2 days (15 CPEs)

Alternative Formats:

This course can be shortened to a one-day introductory class that covers half of the above outline.

[Return to Seminar Listing](#)

AUDITING CHECKPOINT FIREWALLS

Overview:

With increased connectivity to the Internet, organizations can no longer simply rely on operating system security to protect their valuable corporate data. They must also rely on other network security components to provide this protection, including firewalls and routers. These components must be properly configured and managed to ensure that only authorized network traffic is able to pass through to internal networks. This introductory course will help participants understand how firewalls should be configured and managed to provide effective filtering controls for networks. Participants will obtain the knowledge necessary to understand and effectively perform a basic evaluation of firewall configurations and management processes without being overwhelmed with technical details. This course provides control concepts and principles that are generally applicable to any firewall product, as well as principles to apply to an in-depth configuration review of a Check Point NGX firewall.

Audience:

This seminar is targeted towards mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- Network Security Basics
- TCP/IP Internetworking
- Firewall Topologies & Architectures
- Hardening the Host
- Firewall Filtering: Theory
- Firewall Filtering: Practice
- Firewall Administration & Management
- Logging & Monitoring
- NAT & VPN
- Network Security Monitoring
- Auditing CheckPoint NGX – Administration and Management
- Auditing CheckPoint NGX – Security Policy
- Auditing CheckPoint NGX – Logging and Alerting
- Auditing CheckPoint – Advanced Features
- Case Study: Checkpoint NGX

Seminar Duration:

2 days (15 CPEs)

Alternative Formats:

This course can be shortened to a one-day course addressing generic firewall controls.

[Return to Seminar Listing](#)

INTRUSION DETECTION SYSTEMS AND INTRUSION RESPONSE

Overview:

In the security consulting profession, we are continuously tasked with making recommendations about security products. Customers want to know how to make their corporate infrastructure more secure. Years ago, they would ask which firewall to buy, then they wanted a PKI solution, but now it seems that they need to know which intrusion detection system (IDS) to implement. In response to increased market awareness, companies like ISS, Symantec, and CISCO are raking in the revenues for sales of their IDS solutions. Similarly, freeware solutions like Snort are experiencing increasingly frequent download requests. Consequently, intrusion detection has become an important component in the Security Officer's toolbox. However, many security experts are still in the dark about IDS, unsure about what IDS tools do, how to use them, or why they must. This seminar will help answer these questions.

Audience:

IT Auditors, Network Administrators, Security Administrators, and those interested in learning the basics of intrusion detection systems.

Prerequisites:

A basic understanding of general IT concepts

Outline:

- Introduction to Intrusion Detection Concepts
- IDS Architectures
- Intrusion Detection Monitoring
- IDS Maintenance and Operations
- Intrusion Response Planning

Seminar Duration:

1 day (7 CPEs)

NETWORK SECURITY BOOTCAMP FOR IT AUDITORS

Overview:

Organizations can no longer rely on operating system security to protect their valuable corporate data. They must also rely on network security components to provide this protection, including firewalls, routers, VPNs, and intrusion detection systems. These components must be properly configured to ensure that only authorized traffic is able to pass through to internal networks. This seminar will help attendees understand and effectively evaluate the configuration of a firewall, the various components of a Cisco router, the mechanics of encryption and IPSec VPNs, and the different types of intrusion detection systems. This seminar will provide the tools and techniques needed to effectively audit these network security components and determine their effectiveness.

Audience:

This seminar is targeted for mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing and monitoring the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- Network Security Basics
- TCP/IP Internetworking
- Network Security Policy
- Firewall Topologies & Architectures
- Firewall Host Hardening
- Firewall Filtering: Theory and Practice
- Firewall Administration & Management
- Firewall Logging & Monitoring
- Intro to NAT & VPN
- Check Point Admin and Management
- Check Point Security Policy
- Check Point Logging & Monitoring
- Check Point Advanced Features
- Check Point VPN
- Encryption
- Digital Signatures and Certificates
- IPSec VPNs
- Security Issues for VPNs
- Introduction to Intrusion Detection
- IDS Architectures
- Intrusion Detection Monitoring
- IDS Maintenance and Operations
- Intrusion Response Planning
- Introduction to Routers
- Routers and Network Security
- Router Network Interfaces and Routes
- Basic Access Lists
- Advanced Access Lists
- Hardening Router Options and Services
- Terminal Authentication and Access Control
- Security Servers and AAA
- Router Advanced Features
- Router Change & Systems Management
- Router Logging and Monitoring
- An Approach for Auditing Routers
- Network Security Vulnerability Monitoring

Seminar Duration:

5 days (35 CPEs)

Alternative Formats:

This course can be shortened to 1-4 days by covering specific modules.

[Return to Seminar Listing](#)

AUDITING SOLARIS

Overview:

Hardening the operating system is the first, and one of the most fundamental, steps in ensuring that mission critical information is adequately protected on corporate systems. This course will provide a detailed understanding of the security features and configuration settings of the UNIX operating system. During the seminar, we will outline a process for reviewing and auditing the security of UNIX systems to ensure that appropriate countermeasures are in place to protect against common UNIX vulnerabilities, threats, and exploits. The seminar will be focused on Sun Solaris, one of the dominant UNIX variants for mission critical systems that would most often be encountered by an IT Auditor. The seminar will focus on general purpose Solaris configuration issues as well as some optional security features and tools that may be appropriate for highly secure environments, and considers all versions up through and including Solaris 9, as well as some of the key features of Solaris 10. Finally, the seminar will identify and discuss specific audit procedures for reviewing and evaluating the security of Sun Solaris UNIX installations.

Audience:

IT Audit professionals, and others tasked with evaluating controls over UNIX-based systems.

Prerequisites:

A basic understanding of UNIX and general IT concepts

Outline:

- Introduction to UNIX and Solaris
- Users and Groups
- Authentication
- File System and File Permissions
- System Startup and User Initialization
- Internetworking: NFS and Trust
- Network Services
- Logging
- Other Security Controls
- Monitoring

Seminar Duration:

2 days (15 CPEs)

Alternative Formats:

An optional third day is available to provide additional detail on specific network services (mail services, X windows, etc.) and features such as RBAC, sudoers, xinetd, and BSM auditing that may not be used by all organizations.

AUDITING MICROSOFT IIS 6.0

Overview:

This seminar will give participants the knowledge necessary to understand and effectively evaluate controls over web servers running Microsoft's Internet Information Server (IIS) on the Windows 2003 platform. Security controls will be the primary focus of the seminar. The seminar will address general principles and concepts, as well as the detailed technical implementations and configuration settings related to securing and controlling a Microsoft web server. The seminar will also provide "how to" instruction on accessing the control-related settings, files, and other information required to perform an effective risk assessment. This course focuses on the security configuration of the IIS subsystem and will not address the hardening of the underlying host operating system.

Audience:

IT Audit professionals, and others tasked with evaluating controls over Windows IIS servers.

Prerequisites:

A basic understanding of Windows and general IT concepts

Outline:

- Introduction to IIS
- IIS Service Manager Security Settings
- IIS Security
- Hardening Tools
- Securing Active Content
- IIS Logging

Seminar Duration:

1 day (7 CPEs)

AUDITING WINDOWS 2003 SERVERS AND DOMAINS

Overview:

Windows 2003 includes a host of security features that dramatically improves the Windows security posture. However, these new features add a level of complexity that needs to be well understood by those responsible for evaluating its effectiveness. This seminar will outline the steps necessary to ensure that Windows 2003 servers are configured securely. The seminar will address general principles and concepts, as well as the detailed technical implementations and configuration settings related to securing and controlling a Microsoft server. The seminar will also provide “how to” instruction on accessing the control-related settings, files, and other information required to perform an effective risk assessment. Security tools provided with W2K3, including the Security Configuration and Analysis Microsoft Management Console (MMC) tool, Group Policy Management Console, and Security Configuration Wizard, will be discussed in detail.

Audience:

Mid to senior level IT Audit professionals and others tasked with evaluating controls over Windows servers.

Prerequisites:

A basic understanding of Windows and general IT concepts

Outline:

- Service Minimization
- Vulnerability and Patch Management
- Security Policies
- Security Options
- Introduction to Windows Access Controls and Groups
- Access Controls for Files and Folders
- Access Controls for Shares, Registry Keys, and Services
- Windows Event Logs
- Windows Audit Policies and Monitoring
- Other Hardening Controls
- Windows Registry Settings
- Security Monitoring Controls
- Windows Firewall
- Active Directory & Domains
- User and Group Objects
- Group Policy and GPOs

Seminar Duration:

3 days (22 CPEs)

Alternative Formats:

An optional fourth day is also available to provide coverage of additional controls such as AD object permissions and auditing, Remote Desktop and Terminal Services, and Router and Remote Access (RRAS) Services, and permissions for Scheduled Tasks and Printers.

AUDITING ORACLE DATABASE SECURITY

Overview:

This seminar will give participants the knowledge necessary to understand and effectively evaluate security controls over an Oracle database management system. Participants will learn the various security features and options of Oracle and the controls that provide security protection for the Oracle database and the information contained therein. The course will focus on how Oracle databases can be controlled in network-centric and multi-tier distributed application environments and how those controls can be assessed during an audit or security review. This technical course addresses Oracle versions 9, 10, and 11 and the security enhancements that have been introduced in the latest versions of the database.

Audience:

Mid- to senior level IT Audit professionals and others tasked with evaluating controls over Oracle database servers.

Prerequisites:

A basic understanding of general IT concepts

Outline:

- Introduction to Oracle
- Security Architectures for Distributed Systems
- Authentication
- Database Objects
- Privileges: Object and System
- User Roles
- Database Application Security Strategy
- SQL-Plus Security
- Database Links
- System Security Infrastructure
- Logging & Auditing
- Host-level Security
- Oracle Network and Advanced Security

Seminar Duration:

2 days (15 CPEs)

AUDITING WEB SERVER AND WEB APPLICATION SECURITY

Overview:

Security best-practice organizations such as Gartner and ICISA have indicated that 60%-70% of successful hacking attempts were web-based hacks over port 80 that exploited the Common Gateway Interface (CGI) script, web forms, or web server vulnerabilities. Traditional network-based firewalls are unable to prevent or detect these types of attacks. This seminar will focus on the risks and vulnerabilities of web technologies and web applications, as well as the controls needed to mitigate any weaknesses such as command injection, cookie poisoning, and SQL injection attacks. Topics that will be addressed include authentication options, cookies, form fields, data validation, and parameterized SQL. Although the focus of this seminar is on security, transaction integrity will be addressed to some extent as well. This course uses Apache as an example for assessing web server controls. Web application vulnerabilities are discussed in the context of Perl scripts-based applications.

Audience:

Mid- to senior-level IT Audit professionals and others tasked with evaluating controls over Web components.

Prerequisites:

A basic understanding of general IT and web technology concepts

Outline:

- Introduction to Web Technologies
- Web Server Controls
- Web Sessions & and Browser Based Data
- Authentication and Access Controls
- SSL
- Web Privacy Issues
- Apache Web Server
- Web Application Vulnerabilities & Controls
- Preventing Web Application Hacks

Seminar Duration:

2 days (15 CPEs)

Alternative Formats:

A live demo of web application hacks such as SQL injection and form field manipulation is also available for this course. This demo illustrates (using Perl scripts) how the application weaknesses discussed in the course can be exploited. The demo requires shortened Apache and privacy modules. In addition, 1 day versions of this class are available focusing on either the web server or web applications.

AUDITING WIRELESS SECURITY

Overview:

This two-day course will address the fundamental security issues related to WLANs. The focus of the course will be providing an understanding of wireless security concepts and control techniques, along with appropriate technical details to illustrate and expand on these concepts. The course will discuss the basic mechanics of the cryptographic techniques and protocols used in WLANs so that auditors and security professionals will have an ample understanding of the underlying technologies. (This means that this course will contain some highly technical material related to encryption and wireless network frame formats.) Some commonly used WLAN security audit and hacking tools (such as Aircrack) will be discussed at a high-level in the course. However, this class will not provide detailed walkthroughs on how these tools can be used in a security review.

Audience:

IT Audit professionals, and others tasked with evaluating controls over wireless networks.

Prerequisites:

A basic understanding of general IT concepts

Outline:

- Introduction to Wireless Technologies
- Wireless Technology: MAC Layer Details
- Encryption and Integrity: WEP
- Encryption and Integrity: WPA/TKIP
- Encryption and Integrity: RSN/AES-CCMP
- Authentication: Shared, Open, and 802.1x
- Authentication: EAPOL Key 4-Way Handshake and EAP Methods
- Wireless Security Fundamentals
- Other Connection Controls
- Cisco AP Wireless Commands
- Wireless Enumeration and Cracking Tools

Seminar Duration:

2 days (15 CPEs)

Alternative Formats:

This class is also available as a one-day version that excludes coverage of Cisco's implementation, packet flow walkthroughs, and some of the technical details of 802.11i encryption.

ENTITY-WIDE SECURITY MANAGEMENT

Overview:

An entity-wide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. This seminar starts by explaining these concepts as outlined in GAO's Federal Information System Controls Audit Manual (FISCAM), and continues on to discuss areas that have not yet been included in GAO guidance. For each area, the applicable control activities, control techniques, and audit procedures will be discussed in detail.

Audience:

This seminar is designed for entry-level IT Auditors, and financial auditors interested in making the move to IT.

Prerequisites:

None

Outline:

- Information Security Strategy
- Types of Security Risks
- Risk Management Concepts
- Risk Assessment Process
- Auditing the Risk Assessment Process
- Security Policy & Standards
- Hiring, Termination, & Performance Policies
- Security Program Plan
- Security Management Structure
- Security Awareness Training
- Security Monitoring & Evaluation
- Security Incidents
- Incident Response
- Remediation of Information Security Weaknesses
- Vulnerability Assessment
- Contractual Monitoring & Review

Seminar Duration:

2 days (15 CPEs)

Alternative Formats:

This course can be shortened to 1 day by excluding specific modules.

SECURITY ESSENTIALS: INTRODUCTION TO THE CISSP COMMON BODY OF KNOWLEDGE

Overview:

This one-day course will serve as an introduction to the topic areas in the ten domains of the CISSP Common Body of Knowledge as defined by ISC2. SecureIT will address the high-level concepts and issues in each domain. The class is a broad, high-level overview of the information security field. Although this seminar will provide a conceptual understanding of the scope areas addressed by the CISSP exam, the course should not be considered an examination review course.

Audience:

This seminar is designed for entry-level and mid-level IT Auditors with an interest in basic security concepts.

Prerequisites:

None

Outline:

- Access Control Systems and Methodology
- Telecommunications and Network Security
- Security Management Practices
- Application and Systems Development Security
- Cryptography
- Security Architecture and Models
- Operations Security
- Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
- Law, Investigation, and Ethics
- Physical Security

Seminar Duration:

1 day (7 CPEs)

INTRODUCTION TO ENCRYPTION AND PKI

Overview:

As E-commerce grows, many organizations will continue to deploy Public Key Infrastructure (PKI) systems to support encryption, authentication, and non-repudiation services of on-line transactions. This course provides the background on encryption techniques and other components of a PKI system so that auditors can identify the main areas of risk associated with this technology. The course will especially focus on the key risk and control functions provided by Certification Authorities, including generation and protection of keys and revocation of certificates. The importance of the Certification Practice Statement and the role of periodic third party audits (such as the AICPA's WebTrust program for Certification Authorities) will be discussed in the context of RFC 2527 and the American Bar Association PKI Assessment Guide.

Audience:

This seminar is designed for entry-level IT Auditors with an interest in learning about the concepts and controls associated with public key infrastructures.

Prerequisites:

None

Outline:

- Encryption
- Digital Certificates and Digital Signatures
- Introduction to PKI
- Certification Authorities and Certification Practice Statements
- Protecting Key Pairs and Revoking Certificates
- Legal Issues with Non-repudiation and PKI

Seminar Duration:

1 day (7 CPEs)

USING ACL FOR DATA ANALYSIS

Overview:

This seminar, designed specifically for internal and external IT Auditors, will provide the tools and techniques needed to effectively use ACL software to assist in general audit procedures and flexible data analysis requirements. The seminar will begin with a brief session on data acquisition, including the retention and defining of multiple types of data files from disk, tape or ODBC connections. The majority of the course will be spent teaching basic commands and thought processes necessary to complete standard Audit Assistance techniques, including aging, footing control totals, and re-performance of standard audit objectives. Following the completion of these objectives, the course will finish with an overview of some more complicated uses of ACL, including re-performance of depreciation, revenue recognition, and a Journal Entry review.

Audience:

This seminar is designed for IT Audit professionals, and others tasked with verifying the completeness and accuracy of audit-essential control totals and data-intensive corporate processes.

Prerequisites:

None

Outline:

- Introduction: What is ACL?
- Uses of ACL
- Overview of ACL Structure
- Data Acquisition & Definition
- Basic ACL Commands & Functions
- Views, Reports & Graphs
- Sample ACL Projects

Seminar Duration:

1 day (7 CPEs)

CISSP BOOTCAMP

Overview:

This is the premier security certification in the industry today. The CISSP certification is governed by the International Information Systems Security Certifications Consortium (ISC) and gained importance as a key component in the selection process for management-level information security positions. The CISSP certification course was designed to provide a total overview of the Common Body of Knowledge (CBK), the compendium of information security practices and standards compiled and continually updated by (ISC)2 and used as the basis for the CISSP certification exam.

Audience:

This seminar is designed for IT Audit professionals who have at least four years of direct security experience in the field.

Prerequisites:

None

Outline:

- Access Control Systems & Methodology
- Telecom & Network Security
- Security Management Practices
- Applications & Systems Development Security
- Cryptography
- Security Architecture & Models
- Operations Security
- Business Continuity
- Planning & Disaster Recovery Planning
- Law, Investigations & Ethics
- Physical Security

Seminar Duration:

5 days (35 CPEs)

ETHICAL HACKING

Overview:

This class prepares the IT professional to become an Ethical (or WhiteHat) Hacker for their own corporate network environment. Even if your company uses a third party for assessment services, continual testing throughout the year is the only way to maintain the most secure environment possible. This class will provide a solid foundation of ethical hacking methods and procedures to help your IT security staff assess the growing security needs of your environment.

Audience:

This seminar is designed for network server administrators, firewall administrators, system administrators, application developers, and IT security officers.

Prerequisites:

None

Outline:

- Hacking Fundamentals
- Methodologies Review
- Network Scanning & Enumeration
- Network Device Hacking
- Windows Hacking
- Unix/Linux Hacking

Seminar Duration:

5 days (35 CPEs)

COMPUTER FORENSICS

Overview:

Computer crimes have grown significantly as more and more organizations offer an on-line presence to their customers, partners, employees and investors. These attacks can initiate from outside your corporation or from inside your organization's perimeter defenses. When a crime takes place against your organization, it is important to take the appropriate steps to properly discover the evidence that the intruder has left behind and recover lost data. Forensics Training for the Enterprise can help IT professionals prepare their organization to respond to incidents of computer crime.

Audience:

This seminar is designed for network server administrators, firewall administrators, system administrators, application developers, and IT security officers.

Prerequisites:

None

Outline:

- Working Scenarios
- Collecting Digital Evidence
 - Windows Systems
 - Unix/Linux Systems
 - Networking Systems
- Analyzing Digital Evidence
 - Windows Systems
 - Unix Systems
 - Network Traffic
 - Network Devices
- Legal Issues
 - Evidence Collection
 - Law Enforcement Concerns
 - Internet Service Providers
 - Best Practices/Case Studies
- Investigation Practices
 - Real-world compromise tactics
 - Hands-on forensics lab configuration
 - Analysis of common forensics tools

Seminar Duration:

5 days (35 CPEs)

Alternative Formats:

This course can be shortened to 3 days by covering specific modules.

[Return to Seminar Listing](#)