SECURE IT

IT AUDIT AND SECURITY SEMINARS

COURSE CATALOG

SECUREIT CORPORATE OVERVIEW

SecureIT is an information technology (IT) audit and consulting firm dedicated to helping our clients manage technology risks and create business value through effective internal control, information assurance and IT governance practices. By mobilizing teams of highly skilled professionals, SecureIT partners with clients to achieve enduring, measurable results. SecureIT professionals offer unparalleled technical expertise, industry knowledge and managerial skills. They build and share intellectual capital that keeps SecureIT and our clients at the forefront of best practice. SecureIT is committed to serving our clients as a trusted, independent adviser. Our four main service areas are outlined below:

Technology Risk
SecureIT's technology risk consulting services focus on the risk inherent in using information systems to support business objectives. SecureIT's services combine technology expertise, industry knowledge and managerial acumen to help clients manage their technology risks and maximize return on their IT investments through mature governance and control processes. Through our work across multiple industries, SecureIT has acquired expertise introducing best practices to the IT organization, facilitating compliance with laws and regulations, implementing business continuity plans, managing outsourcing risks, and managing the interface between a client's IT organization and its audit entities. Point solutions include:

* Sarbanes-Oxley
* Regulatory Compliance
* Framework (CobiT/ISO/ITIL) Compliance
* Business Continuity Management
* Outsourcing Risk Management
* Audit Readiness
* Audit Liaison Office
* Federal Sector

Information Security
SecureIT offers a comprehensive range of services to help clients assess their threats, vulnerabilities and risks, design and implement information security strategies, and improve their information assurance capabilities through monitoring, periodic reviews, and audits. Our information security services methodology prescribes a risk-based approach to protecting the confidentiality, integrity and availability of information. By taking a holistic approach, SecureIT is able to tailor solutions to our clients' specific needs or facilitate transformation of their information assurance capabilities. Point solutions include:

* Risk Assessment
* Technical Security Reviews
* Penetration Studies
* Enterprise Security Architecture

* Security Program Implementation
* Privacy and Data Protection Back to Top

Internal IT Audit
New laws and regulations, competitive pressure and technological change are placing new demands on internal audit capabilities. The contribution of IT audit (particularly from specialists with a combination of deep technical skills and industry knowledge) is critical to the quality, efficiency and effectiveness of the internal audit function. SecureIT helps clients develop and sustain world-class IT audit capabilities by instituting a risk-based IT audit strategy, performing IT audit projects, and providing ongoing expertise through co-sourcing arrangements. Typically, our IT audit methodology can produce a significant and measurable impact on cost effectiveness of the IT audit function and the value of its contribution to our clients' internal control and corporate governance. Point solutions include:

* IT Audit Planning
* IT Audit Co-sourcing / Outsourcing
* IT Audit Quality Assurance Review
* Infrastructure and Application Audits

Training
SecureIT offers numerous seminars throughout the year, and we deliver custom training programs to our clients. Our goal is to provide high quality, 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 is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors

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 course 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.

- Supplementary materials by request: At each seminar, SecureIT can by request distribute CDs which contain valuable reference materials, links to informative web sites, public audit programs, reference guides, etc.

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, 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 frequently (http://www.secureit.com) as we are constantly adding new courses.

- IT Audit Bootcamp (2 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 Distributed & Web-based Applications (3 days)
- Auditing Solaris (2 or 3 days)
- Auditing Microsoft IIS 6.0 (1 day)
- Auditing Windows 2003 (3 or 4 days)
- Auditing Oracle Databases (2 days)
- Auditing Web Application Security (2 days)
- Auditing Wireless Security (2 days)
- Entity-Wide Security Program Planning & Management (1 or 2 days)
- Auditing with FISCAM (5 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)

SEMINAR OUTLINES

Seminar:
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)

Seminar Name:
Auditing Cisco Routers

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, 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 technical seminar will give participants the knowledge necessary to thoroughly understand and effectively evaluate the configuration of a Cisco router, and case studies will reinforce important concepts learned. This comprehensive seminar will also 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
- An 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.

Seminar Name:
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. Firewalls have emerged as the primary tools used to prevent unauthorized access. Firewalls are placed at the logical borders of an enterprise and aim to prevent unauthorized access to or from the private network. Considering how important these protection mechanisms are, organizations need to ensure not only that they are strategically placed, but also that they are configured in a secure manner. This seminar will give participants the knowledge necessary to understand and effectively evaluate the configuration of a firewall. The industry's leading firewall (Check Point) will be discussed in depth and case studies will reinforce important concepts learned. This seminar will help participants understand the various firewall technologies and give them the tools needed to effectively audit them. Approximately half of this course is general information applicable to all firewalls, and half is focused on applying these concepts to Check Point firewalls.

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 Check Point – Administration and Management
- Auditing Check Point – Security Policy
- Auditing Check Point – Logging and Alerting
- Auditing Check Point – Advanced Features
- Case Study: Checkpoint NG

Seminar Duration:
2 days (15 CPEs)

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

Seminar Name:
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)

Seminar Name:
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, designed specifically for IT Auditors and IT Security professionals, will provide the tools and techniques needed to effectively audit these network security components and determine their effectiveness in an organization's overall security strategy.

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
- Hardening the Host
- Firewall Filtering: Theory and Practice
- Firewall Administration & Management
- Logging & Monitoring
- NAT & VPN
- Check Point Admin and Management
- Check Point Security Policy
- Check Point Logging and Monitoring
- Check Point Advanced Features
- Encryption
- Digital Signatures and Certs
- IPSec VPN
- Security Issues for VPNs
- Introduction to IDS
- IDS Architectures
- Intrusion Detection Monitoring
- IDS Maintenance and Operations
- Intrusion Response Planning
- Introduction to Routers
- Routers & Network Security
- Network Interfaces & Routes
- Basic Access Lists
- Advanced Access Lists
- Hardening Router IOS & Services
- Terminal Line Authentication & Access Controls
- Security Servers & Cisco AAA
- Logging & Monitoring
- Change & Systems Management
- Router Advanced Features
- Summary Approach to Auditing
- Network Security Vulnerability Monitoring

Seminar Duration:
5 days (35 CPEs)

Alternative Formats:
This course can be shortened to 1-4 days by covering only specific modules.

Seminar Name:
Auditing Distributed & Web-based Applications

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

Seminar Duration:
3 days (22 CPEs)

Seminar Name:
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 provides more 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 all organizations.

Seminar Name:
Auditing Microsoft IIS

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)

Seminar Name:
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 provides provided with W2K3, including the Security Configuration and Analysis 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, RRAS services, and permissions for Scheduled Tasks and Printers.

Seminar Name:
Auditing Oracle Databases

Overview:
This seminar will give participants the knowledge necessary to understand and effectively evaluate controls over an Oracle database management system. Participants will learn the various facilities of Oracle and the controls that provide security, integrity, and recovery controls for the Oracle database and the information contained therein. Areas that will be addressed include security architecture, user authentication controls, discretionary access controls, privileged access controls, auditing controls, host operating system controls, database object and transactional integrity controls, and database recovery controls. The seminar will focus on how Oracle databases can be controlled in network-centric and multi-tier distributed application environments.

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
- Integrity, Transactional Integrity, and Recoverability

Seminar Duration:
2 days (15 CPEs)

Seminar Name:
Auditing Web Server and Web Application Security

Overview:
Security best-practice organizations such as Gartner and ICSA have indicated that 60%-70% of successful hacking attempts were web-based hacks over port 80 that exploited 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 addresses 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.

Seminar Name:
Wireless Security

Overview:
This comprehensive seminar will provide attendees with a broad understanding of the security issues that plague Personal Digital Assistant (PDA) and wireless technologies. The session will begin with a brief introduction to PDA and wireless technologies, along with a discussion of their recent advancements. We will then explore the many security issues related to PDAs and wireless devices, particularly as they become more prevalent in corporate infrastructures. Most importantly, we will review how your environment may be at risk and how to mitigate those threats. We will also illustrate how to prevent known vulnerabilities from being exploited. Finally, this seminar will explain how to incorporate PDA and wireless security into an Enterprise Security Program using tools, technology, and policies. The seminar participant should expect to gain insight into the state of PDA and wireless security coupled with "real-world" accounts and useful recommendations from the presenters' industry experiences.

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
- Walkthrough of Wireless Packet Traces

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.

Seminar Name:
Entity-Wide Security Program Planning & 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
- Security Monitoring & Evaluation
- Security Incidents
- Incident Response
- Contractual Monitoring & Review

Seminar Duration:
2 days (15 CPEs)

Seminar Name:
Auditing with FISCAM

Overview:
This seminar will give participants the knowledge necessary to understand and effectively evaluate IT risks and controls in accordance with the Government Accountability Office's FISCAM audit approach. The course outlines and defines basic technical concepts, and provides a risk-based approach for ensuring that adequate controls have been implemented. Modeled after the FISCAM guidance provided by GAO, the class begins at a very basic level and slowly progress into more complex technology issues that are prevalent in today's information processing environments. The seminar consists of modules that address the core areas of IT risk: security management, access control, configuration management, segregation of duties, and contingency planning. Each module will comprehensively discuss each critical element's recommended control activities, control techniques, and audit procedures. Although all requirements of FISCAM will be addressed in the class, additional information based on other Federal control guidance and best practice is incorporated throughout the course. Participants will leave this seminar with a solid knowledge of key IT controls and audit techniques required by FISCAM. The class includes case for each of FISCAM's five domains.

Audience:
This seminar is designed for entry-level and mid-level IT Auditors for government agencies or other auditors that perform GAO-compliant audits.

Prerequisites:
None

Outline:

- Introduction to FISCAM
- Security Management
  - Key Concepts
  - Objectives and Risks
  - Principles of Effective Control
  - Control Activities, Control Techniques, and Audit Procedures
- Access Control
- Configuration Management
- Segregation of Duties
- Contingency Planning
- Applying FISCAM to real life audits
- Case studies

Seminar Duration:
5 days (35 CPEs)

Seminar Name:
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)

Seminar Name:
Introduction to Encryption and PKI

Overview:
As E-commerce grows, many organizations will continue to deploy a 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)

Seminar Name:
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)