

Control & Security of Enterprise Wide E-Commerce

COURSE DURATION: 2-days

CPE HOURS: 16

LEVEL: Beginner / Group-Live

PREREQUISITES: None

ADVANCE PREPARATION: None

This seminar is intended to provide auditors and security officers with a complete audit and security approach to the E-commerce environment that spans the enterprise. The author (Gordon Smith) has over 28 years of technical IT audit experience and has summarized a lifetime of experience into creating a proven audit and security approach to E-commerce. Based on his new book (Control and Security of E-commerce, John Wiley and Sons), the seminar provides a detailed understanding of E-commerce risks and how to mitigate them. Each module provides a complete understanding of audit and security concerns and provides practical and affordable solutions to ensure that your organization's E-commerce site is safe and secure. Each of the audit and control modules contains a full set of risk / control tables that identify specific issues and the controls required to prevent or mitigate them (over 50 pages in total). Also included is a series of COSO compliant control checklists (over 35 pages in total) that can be used to quickly identify the E-commerce business issues. In addition, the participants in this seminar will be **granted access to the special E-commerce section of the Canaudit Web site**. Here they can download electronic copies of the full audit guide and other useful tools to evaluate and secure their E-commerce environment.

WHO SHOULD ATTEND

This seminar is designed for auditors, security officers and business professionals.

SEMINAR OUTLINE

I Introduction

- Evolution of E-commerce
- Brick and click versus dot.gone
- Fully integrated web commerce
- E-commerce functionality
- Cyber crime and other threats
- Business globalization through E-commerce
- Practice business examples

II Information Security in the E-Commerce World

- Security issues abound! Choosing the right battle!
- SAS-70 reports – can you rely on them?
- Business continuance and fail over mechanisms
- Electronic theft and corporate espionage
- Protecting confidential client information
- Denial of Service attacks, Trojan programs and back doors
- Software failure
- Hardware and network failure
- Human error
- Cryptography and Encryption
 - Symmetric and asymmetric cryptosystems
 - Key management and transfer techniques
- Digital Signatures and other techniques
- Risk / control tables
- Audit checklists

III Protecting the E-Commerce Environment

- Safe and sane design concepts
- Using zones to enhance security
 - The Internet zone
 - The Extranet zone
 - The Intranet zone
- Building, configuring and protecting the firewalls
- Understanding and controlling port access
- Control and security of VPN's
- Secondary authentication techniques
- Protecting your E-commerce servers
- Risk / control tables
- Audit checklists

IV Protecting E-Commerce Data

- Ending misconceptions of "Internet theft"
- The outward approach to data security
- Securing the data
- Securing the operating systems
 - Securing Unix
 - Securing Windows
- Network security
- Risk / control tables
- Audit checklists

V Legal Issues Relating to E-Commerce

- Legal changes to facilitate E-commerce
- Contracts and agreements

- Acceptance and proof of delivery
- E-commerce in the courtroom
- Business records on trial risk / control tables
- Creating good E-commerce contracts
- Risk / control tables
- Audit checklists

VI Certificates and Non-Repudiation

- Digital certificates
- Certificate authorities
- Issuing and controlling certificates
- Non-repudiation: Requirements for Internet business
- Risk / control tables
- Audit checklists

VII Auditing an E-Commerce Application

- Overview of the application
- The audit guide
- Process analysis
- Anticipated controls
- Risk assessment
- Identifying potential Fraud
- Items with cash flow potential
- Risk / control tables
- Audit checklists

VII Wrap Up