

Control and Security of Enterprise-Wide E-Commerce

Course Duration: 2 Days
CPE Hours: 16 Hours
Level: Beginner/Group-Live
Prerequisites: None
Advanced Preparation: None

This two-day 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 of the course material, Gordon Smith, has over 30 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 book, Control and Security of E-Commerce (John Wiley and Sons), this seminar provides a detailed understanding of the e-commerce risks and how to mitigate them. Each module provides a complete understanding of audit and security concerns and practical and affordable solutions to ensure an 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. Also included in the material is a series of COSO-compliant control checklists that can be used to quickly identify e-commerce business issues. In addition, participants of this seminar will be able to download electronic copies of the full audit guide from our website 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 vs. 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 failover mechanisms
- Electronic theft and corporate espionage
- Protecting confidential client information
- Denial of Service attacks, Trojan programs and backdoors
- 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 VPNs
- Secondary authentication techniques
- Protecting your e-commerce servers
- Risk/Control tables
- Audit checklists

IV) Protecting E-Commerce Data

- Ending misconceptions about "Internet theft"
- 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
- 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

VIII) Wrap Up