



AEC100 Audit & Control Considerations in Electronic Commerce

CPE 7.0

Description: This seminar provides insight to those professionals who have grappled with electronic commerce and information security issues surrounding the continued growth of virtual markets. Electronic Commerce (EC) is a range of applications that extends the core business activities of the enterprise into a virtual electronic community that is shared with customers, suppliers, business partners, employees, and prospects.

Connecting businesses and consumers, be it for banking, retail sales, or confirming airline reservations, controlling electronic commerce (EC) will require an integrated examination of electronic data interchange (EDI), electronic funds transfer (EFT), electronic benefits transfer (EBT), and the Internet. Unsecured electronic commerce presents risks which could create a 'black hole' of liability for organizations, seminar attendees will be prepared for the challenges of auditing, assessing and securing automated financial electronic commerce applications, with an aim of avoiding such corporate liabilities.

Audience: This seminar is intended for internal and external audit professionals, Controllers and their management, system developers, Chief Technology Officers, Chief Information Officers, Chief Security Officers, and individuals who wish to learn more about securing and controlling their organization's electronic commerce environment.

Prerequisites: There is no prerequisite for this seminar. No advanced preparations are required for this seminar.

Objectives: After completing this seminar, participants will be able to:

- Identify the various uses of Internet technology and that the changing roles of this technology in an e- business environment can jeopardize the reliability of information both from a management and an audit point-of-view.
- Evaluate E-commerce risk assessment and controls.
- Determine that an e-business organization faces new threats to the safeguarding of its assets, and that the access to those assets is often managed via IT-systems. Further, manipulation of those systems could lead to unauthorized use of assets.
- Identify that access controls, log files and segregation of duties are key controls in maintaining overall security in emerging virtual markets governed by E-commerce.
- Perform an audit of their organization's E-commerce environment.



**Business
Automation
Consultants, LLC**

IT Audit Training, Security Reviews and IT
Management Consulting Services -- Since 1984

Course Outline:

Leveling the Playing Field: A Quick Look at the Internet Numbers

Defining Electronic Commerce

- Elements of Electronic Commerce
- Goal of E-Commerce

Electronic Commerce - Setting a Course for Success

- E-Commerce vs. E-Business
- The E-Business Cycle

Rise of the Internet Economy's "Net" Impact

- Critical Issues in E-Commerce

Functional Parts of Electronic Commerce

- Key Factors to E-Commerce Development Processes
- Emerging E-commerce Business Models
- VPN Security and Control

EC Risks

- Threats to E-Business

Auditing Electronic Commerce

- EC Security Considerations
- Securing Web Architecture Design

Establishing Trust in Virtual Markets

- Building Credibility
- Why Does Web Credibility Matter?
- Building Trust
- EDI and EC

Secure E-commerce Options

Electronic Data Interchange- Audit and Control Issues

- EDI: Nine Areas of Audit Concern
- Performing an EDI Audit

General Electronic Commerce Security Tools

Specific Electronic Commerce Security Tools

Utilizing E-Commerce Audit "Tools and Techniques"

- Mistakes to Avoid in Planning a Successful E-Commerce Strategy

Privacy and Identity Theft

Dr. Marcella's seminar is based on findings from his books; Electronic Commerce: Control Issues for Securing Virtual Enterprises, and Establishing Trust in Virtual Markets, published by the Institute of Internal Auditors, and EDI Security, Control and Audit, published by Artech House.

www.businessautomationconsultants.com/published-books.html