

I.S. Auditing for Integrated Auditors

COURSE DURATION: 2-days

CPE HOURS: 16

LEVEL: Beginner / Group-Live

PREREQUISITES: None

ADVANCE PREPARATION: None

This seminar is targeted to integrated or financial auditors who will be performing a general controls review of a small data center or a series of local area networks. They will gain an understanding of the risks facing small and medium sized data centers, and the controls required to mitigate these risks. In addition, participants will learn the Canaudit Cooperative Audit Approach for the general controls audit. This COSO compliant approach uses a series of checklists to assist in information gathering and documenting critical information system controls before the field work begins. The field work consists of interviews and audit testing to provide solid examples of control weaknesses. A series of risk/control tables, which are provided for each audit module, helps auditors to summarize the risks, suggest viable controls, and facilitate reporting of audit issues. Coverage includes physical security, logical security and access control, administrative procedures, backup, recovery, and business continuance. This is the perfect how-to primer for auditors embarking on their first review of small LANs or small to medium sized data centers.

WHO SHOULD ATTEND

This seminar is intended for integrated or financial auditors who will be performing a data center audit. It is also ideal for I.S. auditors with less than six months experience.

SEMINAR OUTLINE

I. Introduction

- Requirements for a general controls audit
- Physical security hazards
- Doors, locks and person traps
- Automated entry systems
- Managing physical access
- Risk/Control Tables
- Audit checklists
- Audit program

II. Physical Security

- Physical access controls
- Rule of least access
- Physical security hazards
- Doors, locks and person traps
- Automated entry systems
- Managing physical access
- Risk/Control Tables
- Audit checklists
- Audit program

III. Logical Security and Access Control

- Data ownership versus security
- Confidential information
- Securing data in a multi-platform environment
- Granting access to groups and users
- Access control techniques
- Monitoring access violations
- Monitoring successful access
- Risk/Control Tables
- Audit checklists
- Audit program

IV. System Administration

- User and group administration
- System administration
- Data administration
- Neighbor maintenance
- Software administration
- Backup and recovery
- Resource management
- Risk/Control Tables
- Audit checklists
- Audit program

V. Backup and Recovery

- Identifying required backups
 - System backups
 - Incremental backups
- Verification of backups
- Offsite and remote requirements
- Restoration procedures
- Risk/Control Tables
- Audit checklists
- Audit program

VI. Business Continuance and Disaster Preparedness

- Building fault-tolerant applications
- Building fault-tolerant systems
- Disaster prevention
- Disaster containment
- Disaster Recovery
- Risk/Control Tables
- Audit checklists
- Audit program

VII. Reporting Techniques

- Shortening the reporting timeframe
- Building the report
- Exit interview techniques