



27 Pine Street, Suite 700
New Canaan, CT 06840
Phone: (203) 972-3567 Fax: (203) 972-3367
e-mail: Levinemh@auditserve.com Website: <http://www.auditserve.com>

Audit Seminars

IT Controls Required to Enforce Data Privacy and Prevent Fraud

Seminar Objective

Regardless if your interests relate to the Government, Health Care, Retail or Financial industries, this seminar cuts across all of the data privacy and fraud detection/prevention legal requirements in order to establish implementation and audit validation requirements.

Seminar Length

One Day

Delivery Method

Group-Live

Prerequisites

Minimum of two years IT or Operations Audit Experience

Program Level

Intermediate

Continuing Professional Education Credits



Audit Serve 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. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding sponsors may be addressed to National Registry of CPE Sponsors, 150 Fourth Avenue North, Suite 700, Nashville, TN 37219-2417, USA Web site: www.nasba.org.

CPE Credits: 8

CPE Field of Study: Accounting and Auditing

IT Controls Required to Enforce Data Privacy and Prevent Fraud

Contact Information for Complaints

To register a complaint, please contact our Customer Service Department at (203) 972-3567.

Refund/Cancellation Policy

For seminar locations within the New York, New Jersey and Connecticut areas there is no cancellation fee as long as notification is received by phone or e-mail 5 or more business days prior to the scheduled seminar date. Otherwise, there is a \$500 cancellation fee.

Seminar Outline

I. Introduction to Data Privacy and Fraud Prevention

- What is PHI, PII and private employee & customer information?
- Data Privacy & Fraud Prevention Legal Requirements
 - How these legal requirements impact specific industries
- Security and operational impacts of recent legislation (HITECH Act and others)
 - How companies are addressing these requirements

II. Alternative Approaches to establishing Risk Assessment

III. Establishing and Auditing a Privacy Impact Assessment

IV. Data Classification Standard

- Alternative approaches used for developing a data classification standard
- Implementation requirements
- How to audit a data classification standard

V. Fraud Detection & Prevention

- Detective controls used to prevent fraud
- Automating detective review processes
- Alternative audit trails
- Preventive controls used to prevent fraud

VI. Third Party Relationship handling

- Business partner data exchange
- Handling third-party vendor access

IT Controls Required to Enforce Data Privacy and Prevent Fraud

Seminar Outline (continued)

VII. Reassessment of Access Control Requirements

- Upgrade requirements to logon security
- Security design approaches which do not meet Data Privacy and Fraud Prevention requirements
- Disclosure of data control strategies

VIII. PCI Compliance

- Key initial project steps
- PCI scope reduction strategies
- PCI project show stoppers
- An insiders view of how to become and maintain PCI compliance
- Unpublished methods to resolve “show stopper” non-compliance issues
 - Realistic measures for maintaining confidentiality of data in transit
 - Alternative approaches for securing data at rest
 - and a few more tricks

IX. Case Study

- Data classification, data privacy & fraud prevention case study (Payroll Processing)