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.

Participant Learning Objectives

At the completion of the seminar, the following learning objectives will be achieved by all participants:

- Be able to conduct interviews in order to identify data privacy issues and IT controls required to prevent fraud
- Be able to conduct a Data Privacy Assessment
- Be able to establish and implement a Data Classification Standard
- Be able to establish an enterprise and application-level Risk Assessment
- Be able to identify key issues within an environment preparing to be PCI compliant

Seminar Length

Two days

Delivery Method

Group-Live or Group Internet-Based

Prerequisites

Minimum of two years IT, Security or Audit Experience

Who Should Attend?

Auditors, Security Administrator, Quality Assurance personnel and Fraud Examiners

Program Level

Intermediate

IT Controls Required to Enforce Data Privacy and Prevent Fraud

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: 15
CPE Field of Study: Auditing - General

Contact Information for Complaints

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

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. Data Privacy Approaches for Government Agencies

- Implementation and compliance approaches
  - H.R. 516 Federal Agency Data Privacy Protection Act
  - Privacy Provisions of the E-Government Act of 2002
  - FISMA Act of 2002
  - Privacy Act of 1974
  - Inter-Agency Sharing of Personal Data
- How to conduct privacy impact assessments

III. Risk Assessment processes

IT Controls Required to Enforce Data Privacy and Prevent Fraud

Seminar Outline (continued)

IV. Establishing and Auditing a Privacy Impact Assessment

V. Data Classification Standard

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

VI. Fraud Detection & Prevention

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

VII. Third Party Relationship handling

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

VIII. 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

IX. Entity-level controls used to foster data privacy and fraud prevention

- Spreading data privacy within security awareness programs
- Corporate Policies, standards and methodologies
- Alternative roles of compliance functions

X. 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 ……

XI. Case Studies

- Data classification, data privacy & fraud prevention case study (Payroll Processing)
- Data privacy & fraud prevention case study (Hotel operations)
- Fraud prevention case study (Purchase Requisition)