

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.

CPE Credits: 8

Instructor & Organizer's Biography Mitchell H. Levine, CISA

Mitchell Levine is the founder of Audit Serve, Inc. which is an IT Audit & Systems consulting company. For the last 20 years at Audit Serve, Mr. Levine has split his time between traditional IT & Integrated Audit Consulting projects, PCI Implementations, SOX Implementation/Testing Projects and the implementation of defect tracking, compliance and software management systems. Mr. Levine spends 220+ days per year consulting which is the basis for the material which is included in the seminars.

Over the past five years Mr. Levine has presented over 35 seminars to thirteen different ISACA & IIA chapters. Mr. Levine also was the primary writer and editor of the Audit Vision Magazine which was published from 1991 – 1998. The magazine was transformed into the Audit Vision E-mail newsletter which is published monthly which has a subscription base of over 3,500 audit & security professionals.

Prior to establishing Audit Serve, Inc. in 1990, Mr. Levine was an IT Audit Manager at Citicorp where his duties included managing a team of IT Auditors who were responsible for auditing 25+ service bureaus and the corporate financial systems.

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 operation impacts of recent legislation (HITECH Act and others)
 - How companies are addressing these requirements

II. Risk Assessment processes

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. Detective Processes “red flags”

- Alternative audit trails
- Evaluating Detective Process “red flags” to reduce Fraud
- Identifying inadequate data collection processes
- Automating detective review processes

VI. Third Party Relationship handling

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

VII. Reassessment of Access Control Requirements

- Upgrade requirements to logon security
- Security design approaches which do not meet Data Privacy and Fraud Prevention requirements
- Realistic measures for maintaining confidentiality of data in transit
- Alternative approaches for securing data at rest

VIII. PCI Compliance

- An insiders view of how to become and maintain PCI compliance
- Unpublished methods to resolve “show stopper” non-compliance issues