AUDIT
SERVE INC.

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

IT Audit Seminars

Managing and Auditing Cybersecurity – Data, Infrastructure and Applications

The seminar for experienced audit professionals

Seminar Objective/Background

After being on the audit side for the first half of his career 30 year career, the instructor has spent most of the last 15 years consulting full-time with systems development groups, Infrastructure groups and data centers, uncovering many cybersecurity control issues which were in many instances unknown to the most experienced auditors. The instructor has devised unique methods for performing compliance testing which disclose major gaps in an organization’s control design.

Seminar Length

One day (7 hours plus 1 hour lunch and two 15 minute breaks)

Who Should Attend

This seminar is designed for senior IT Auditors.

Learning Outcomes

Attendees will achieve the following learning outcomes:

- Will be able to identify the production resources which need to be included in-scope for a security access audit
- Understand the controls that need to be established to prevent traditional access controls from being bypassed
- Identify key network security design initiatives required to prevent cyber security attacks
- Understand the key components to performing an effective data privacy audit
- Understanding the control requirements within a mid-tier environment
- Effective methods for implementing a Cybersecurity program
- Understanding how new regulations are raising the bar of the expected requirements of a cybersecurity program

Seminar Outline

The following topics, system practices and schemes will be discussed:

- Cybersecurity overview

- Understanding the recent cybersecurity regulations and how they are raising the bar of the required security controls

- Implementing a Cybersecurity program using the NIST and other frameworks

- Recent introduced Cybersecurity related frameworks
  - NIST.SP.800-207 (Zero Trust Architecture)
  - NIST 8374 (Cybersecurity Framework Profile for Ransomware Risk Management)

- Conducting Cybersecurity & Data Privacy Audits/Assessments
  - Alternatives to approaching the Cybersecurity Audits
  - In-depth auditing techniques for Cybersecurity focus areas
    - Network Security
    - Host-level Security
    - Database security
    - Application and mid-tier security
    - Control of PII
    - Data Loss Prevention

- Understanding and designing programs to prevent current cyber-attack trends

- Implementing and auditing Incident Management and Data Breach Handling processes which includes enhances requirements mandated by GDPR and other data protection regulations

Seminar Length

7 ½ hours plus four two minute breaks and 1 hour lunch

Field if Study

Auditing

Prerequisites

Basic knowledge of Auditing.

Field if Study

Auditing

Advanced Preparation

None

Program Level

Intermediate

Continuing Professional Education Credits

The seminar is structured to allow ISACA and IIA chapters to issue 8 CPEs.

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 28 years at Audit Serve, Mr. Levine has split his time between traditional IT & Integrated Audit consulting projects, Conducting cybersecurity assessments, restructuring IT Departments, Implementing DFS Part 500 Cybersecurity initiatives, PCI Implementations, and performing pre & post-implementation reviews of system migrations. Mr. Levine spends 220+ days per year consulting which is the basis for the material which is included in the seminars.

Over the past sixteen years Mr. Levine has presented over 110 seminars to twenty-seven different ISACA & IIA chapters. Mr. Levine also was the primary writer and editor of Audit Vision which is published monthly and has a subscription base of over 3,000 audit & security professionals.

Prior to establishing Audit Serve, Inc. 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