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

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 cyber security programs.

Seminar Length

Two days (7 ½ -hour presentation time per day plus 1-hour lunch and four 10-minute breaks per day)

Who Should Attend

This seminar is designed for senior IT Auditors, Security and GRC personnel.

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.

For locations outside the New York, New Jersey and Connecticut areas there is a $500 cancellation fee for seminar which covers non-refundable flights. If cancellation notice received less than 3 days prior to the event there is an additional $180 cancellation fee to cover one-night hotel cancellation fee.

Continuing Professional Education Credits

All attendees are eligible to receive 16 hours of continuing professional education (CPE) credits by attending. These credits are recognized by the National Association of State Boards of Accountancy (NASBA). The CPE field of study is Accounting and Auditing. No prerequisites or advanced preparation is required. 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 (615) 880-4200 Web site: www.nasba.org.

Managing and Auditing Cybersecurity – Data, Infrastructure and Applications

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, host-level, database and application design initiatives required to prevent cyber security attacks
- Understand the key components to performing an effective data privacy audit
- 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 will be discussed:

Day 1

- Cybersecurity overview
- Understanding the recent cybersecurity regulations and how they are raising the bar of the required security controls
- Detailed implementation and audit guidance for DFS Part 500 Cybersecurity Requirements for Financial Institutions, how they are being adopted by other states, and how the March 1, 2019 deadline to complete vendor due diligence oversight programs are impacting many organizations across the US
- Implementing a Cybersecurity program using the NIST and other frameworks
- Establishing models to drive decision making processes for security technology to be deployed
- Cybersecurity approaches when using third party service providers

Day 2

- Conducting Cybersecurity and Data Privacy Audits
    - 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

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

- Understanding how controls over production access are being bypassed

- Ineffective security design & management approaches

Case Studies

Two case studies (i.e., one each day) will be presented during the seminar which will provide the attendees the understanding of how to identify flaws within an organizations cybersecurity program and how to establish effective compliance testing.

Audit Program

An audit program which covers all topics discussed will be distributed as part of the session materials.