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

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.

Continuing Professional Education Credits

The seminar is structured to allow ISACA and IIA chapters to issue 15 CPEs.

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
- Will understand how to perform an audit of a NIST 2.0 implementation

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
- Implementing a Cybersecurity program using NIST 2.0 (updated for latest version of 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)
- 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 & Data Privacy Audits/Assessments
  - Alternatives to approaching the Cybersecurity Audits
  - In-depth auditing techniques for Cybersecurity focus areas
    - Network Security (i.e., which includes network segmentation to isolate malware attacks and security approaches used within a cloud and on-premises environments)
    - 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
- 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 a proper incident response plan.

Audit Program

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