



27 Pine Street, Suite 700  
New Canaan, CT 06840

Phone: (203) 972-3567 Fax: (203) 972-3367

e-mail: [Levinemh@auditserve.com](mailto:Levinemh@auditserve.com) Website: <http://www.auditserve.com>

## IT Audit Seminars

### GDPR Implementation, Assessment, and Auditing Approaches

#### Background

Organizations are transitioning to the post-rollout phase of the GDPR project in which they are performing self-assessment of whether they took the initiatives to the appropriate level as compared to their peers.

This seminar has been restructured based on the May 25<sup>th</sup> rollout to evaluate approaches used within the industry for handling the disclosure, lawfulness of processing (e.g., Legitimate Interest, expressed consent), access/deletion practices and overall SAR Request handling which will provide a basis for organizations to adjust their project approaches. For auditors who have been asked to push back their GDPR Audits to allow for the GDPR project team to meet the May 25<sup>th</sup> rollout, now is the time to schedule these post-implementation audits to assess the risks taken by their organizations based on their project strategies.

#### Seminar Length

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

# GDPR Implementation, Assessment, and Auditing Approaches

## Seminar Objective

This GDPR seminar has been restructured to provide attendees a consolidated view of how to implement, assess and audit the project. This seminar is intended to provide attendees the base level knowledge required to (1) conduct a “point-in-time” Assessment to provide a basis to determine the current stage of GDPR compliance and identify the remaining project initiatives, (2) manage the implementation of the GDPR project, and (3) conduct a GDPR Post-Implementation Audit.

## Detailed Seminar Outline

### I. Brief background on GDPR

- Who is impacted?
- Key players within GDPR
- Terminology
- High level introduction of key regulations

### II. Understanding and evaluating the key Regulations from an Implementation, Assessment and an Audit standpoint

- Understanding the required components Record of Processing Activities (Article 30)
  - Properly defining purpose of processing
  - Categories of data subjects
  - Categories of personal data transfer mechanisms
  - Retention periods
- Evaluating whether proper disclosures have been established for types of data subjects which meets Article 13 & 14 disclosure requirements
  - How data from Record of Processing Activities ties to the Article 13 & 14 disclosures processes
  - Evaluating Privacy Policies and ePrivacy (Cookie Law) to ensure disclosures are properly defined
- Understanding and the alternative approaches for Article 6 Lawfulness of Processing
  - Legitimate Interest
  - Expressed Consent
  - Contract

# GDPR Implementation, Assessment, and Auditing Approaches

## Detailed Seminar Outline (continued)

- Establishing and auditing a Legitimate Interest Assessments
- Managing Expressed Consents
- Buildout and Operationalization of Subject Access Rights (SAR) Requests
  - Right to Access (Articles 15)
  - Right to Recertification (Article 16)
  - Data Portability (Article 20)
  - Right to Erasure/Right to be forgotten (Article 17)
  - Right to Object to Processing (Article 21)
- Establishing Data Removal Processes to Support Article 25
- Processor GDPR Business Integration and compliance validation
- Evaluating mechanisms used to meet Article 32 Requirements
  - Utilization of existing certifications
  - Risk Assessment processes
  - Information security policies, procedures and standards which are consistent with the Privacy Shield security principles
- Assessing proper use of Cross Border data transfers for moving data outside of the EU

# GDPR Implementation, Assessment, and Auditing Approaches

## Who Should Attend

The seminar for mid-level IT (including GDPR project managers), GRC and audit professionals but would also be highly invaluable for Senior Management who need to understand the scope of this project and how it impacts their organizations

## Continuing Professional Education Credits



All attendees are eligible to receive 8 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](http://www.nasba.org).

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

Mitchell Levine, CISA is the founder of Audit Serve, Inc. which was established in 1990. For the last 28 years at Audit Serve, Mitch has split his time between traditional IT & Integrated Audit Consulting projects and global project initiatives. For the past two years Mitch has been focusing most of his time on the GDPR project in which he has presented his GDPR seminar 13 times in the last 9 months in which three of these presentations occurred in Europe. He has completed GDPR Impact Analysis & Assessment projects for three separate organizations, conducted an implementation for multi-national organization with over 300k in-scope data subjects, conducted an audit of a large organization with 5 million in-scope data subjects and is currently on two long-term client engagements implementing GDPR initiatives.