27 Pine Street, Suite 700
New Canaan, CT 06840
Phone: (203) 972-3567 Fax: (203) 972-3367
e-mail: Levinemh@auditserve.com Website: http://www.auditserve.com

IT Audit Seminars

Conducting a GDPR Post-Implementation Audit & Assessment

Background and Seminar Objective

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. For some organizations a risk-based approach was taken in which not all the project initiatives have been completed to meet all the articles set forth within GDPR.

The Post-Implementation Audit of the GDPR project is the most critical auditable entity in the Audit Universe for 2019. This audit is the most difficult audit to be performed because there is subjectivity to how far the project initiatives must be taken in order not to be cited by the Supervisory Authority for non-compliance. Conducting a Post-Implementation Assessment of the GDPR project is different from an audit because the person conducting the assessment must have the background in order to evaluate whether an organization has taken the project initiatives far enough to meet a strict interpretation of the articles set forth within GDPR.

This seminar material is based on the instructor's unique experience in conducting several GDPR implementations prior to the GDPR effective date and conducting five post-implementation audits since the effective date.

From this seminar an auditor will be able to assess the risks taken by their organization based on their project implementation strategies and understand how to construct the compliance tests necessary to yield the most compelling audit issues.

This is a completely new seminar established from the perspective of providing auditors the necessary knowledge to conduct a GDPR Post-implementation Audit and consultants to perform an effective GDPR Post-implementation Assessment.

Seminar Length

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

Conducting a GDPR Post-Implementation Audit & Assessment

Detailed Seminar Outline

- Brief background on GDPR
    - Who is impacted?
    - Key players within GDPR
    - Terminology
    - High level introduction of key regulations
- Understanding and auditing 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
- Establishing and auditing a Legitimate Interest Assessments
- Managing Expressed Consents
- Auditing and Assessing the 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)

Conducting a GDPR Post-Implementation Audit & Assessment

Detailed Seminar Outline (continued)

- Assessing the Data Removal Processes to Support Article 25
- Assessing the 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

Who Should Attend

The seminar for mid-level IT (including GDPR project managers), GRC, GDPR consultants and audit professionals.

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.

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 2 1/2 years Mitch has been focusing most of his time on the GDPR project conducting several consulting projects for three separate organizations implementing solutions to meet the requirements set forth within GDPR which included the performance of several GDPR Assessments. Mitch successfully presented his last GDPR seminar entitled "GDPR: Assessment, Implementation and Auditing Approaches" to 12 ISACA local chapters. Mitch has conducted post-implementation audits for five business units since the May 25, 2018 GDPR effective date which forms the basis of the materials presented for this seminar.