IT Audit Seminars

Hidden Secrets From IT Auditors 2015 Edition
The seminar for experienced IT audit professionals

Seminar Objective

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 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
Two days (7 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.

Continuing Professional Education Credits

All attendees are eligible to receive 15 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.

Hidden Secrets From IT Auditors 2015 Edition

Seminar Outline

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

- Conducting Cybersecurity Audits

  - Using the NIST framework to implement a Cybersecurity program
  - Alternatives to approaching the Cybersecurity Audits
  - In-depth auditing techniques for Cybersecurity focus areas
    - Network Security
    - Control of PII
    - Incident Response
    - Data Loss Prevention

- Understanding how controls over production access are being bypassed

- Ineffective Security Design & Management

- Performing an audit of Mid-Tier systems

  - Biz Talk and BEA Audits
    - Message-level security
    - Message-queue security

- Conducting a SharePoint Audit

- Auditing IT Outsourcing Audits

- Auditing Data Warehouses

- Limitation of controls within a SaaS (Software as a Service) application deployment

- Techniques used to bypass the requirements of the SDLC

- Conducting an IT Cost Management Audit

and a few other tricks of the trade…

For each of the above topics, the following will be discussed where appropriate:
• What it is and reasons for its occurrence
• Examples of how it is set-up
• Steps to determine whether it is used within your organization
• Establishment of preventive controls
• Alternative compliance test techniques