

Detecting Fraudulent Financial Reporting Using Data Analysis

What motivates individuals to prepare fraudulent financial statements? Tax evasion? Money laundering? Skimming? Although their motivations are virtually limitless, the techniques available to auditors and investigators to detect these frauds are amazingly similar.

This one-day seminar will provide participants with hands-on training in techniques to detect a variety of frauds, including sales misstatements, skimming, billing schemes, payroll schemes, and expense reimbursement schemes. Participants will perform these techniques using Microsoft Excel and Access and selected techniques will be demonstrated using ACL and IDEA.

Examples of data analyses to be performed include:

- Detection of shell companies by the
 - (1) Comparison of related party (owners and employees) initials with vendor names.
 - (2) Comparison of related party addresses with vendor addresses.
 - (3) Search of missing or inconsistent vendor data.
 - (4) Identification of increasing frequency of checks written.

- Search for unusual transactions by the
 - (1) Search of debit transactions to natural credit accounts (for example, to reduce sales).
 - (2) Search of sales transactions for no corresponding inventory or commission transactions.
 - (3) Search for transactions ending in unusual numbers (0.00 or 9.99)
 - (4) Search for increasing costs of products and services.
 - (5) Application of Benford's Law to identify unusual activity in accounts.

- Search for record manipulation by the
 - (1) Search for missing transactions.
 - (2) Search for out-of-sequence transactions.
 - (3) Search for transactions made to accounts via journal entries from related parties.

The instructor, Dr. Mark W. Lehman, CPA, has taught at Mississippi State University since 1984 and has been teaching and researching in the area of fraud examination for over eight years. He currently teaches the graduate course Fraud Examination and is the author of the seven fraud-related articles and one textbook.