



The Mechanics of Analysis for Fraud Detection

Part III: Best Practices

Before you can fight fraud, you need to understand it and its impact to your organization's bottom line.

According to the ACFE's 2008 Report to the Nation on Occupational Fraud and Abuse, occupational fraud is defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets".

ACL Audit Analytics technology is used by many leading companies as their primary tool in fighting fraud because it's proven, efficient, and helps find money that is lost to fraud, error and abuse.

This white collar crime makes a huge impact on the economy: 7% of an organization's annual revenues according to this report. Now more than ever, it's critical to minimize potential revenue leakage through fraudulent activities and mitigate business risk.

So – what can you do to fight fraud and prevent financial loss?

The first thing to keep in mind is the rule of continuous monitoring: to effectively test and monitor internal controls, organizations must analyze all relevant transactions against control parameters, across all systems and all applications. Only by examining transactions at the source level, can you be assured of the integrity and accuracy of the information.

If 7% loss of revenue sounds high for your organization, then consider what is 1% of the yearly revenue? If this amount is significant, then consider these Six Best Practices in Data Analysis for Fraud.

1) Build a profile of potential frauds. This profile includes a list of the many different areas in which fraud may occur and the types of fraud that are possible in that area; it can be further developed as part of your overall risk assessment.

2) Test data for possible indicators of fraud. A complete testing program should include ad hoc testing in addition to more formalized or regular tests. The spectrum of automated testing ranges from ad hoc through to repetitive through to continuous.

3) Improve the process by implementing continuous analysis. Use continuous analysis to test and validate the effectiveness of your controls and identify

fraud indicators – on a timely basis. Provide management with immediate notification, create processes for control remediation, and implement on a comprehensive basis across business process areas.

4) Review results from testing and continuous analysis. Investigate patterns and indicators that emerge from fraud detection tests and continuous analysis. Quantify the risk of fraud, identify and target those high risk areas, and consider creating a risk monitoring dashboard.

5) Expand scope and repeat. This process of building a profile, testing data, improving controls and reviewing information needs to be done on a regular basis.

6) Report. Offer recommendations on how to tighten controls or change processes to reduce the likelihood of fraud recurrence. Then follow-up and ensure those recommendations have been acted upon and have had the desired effect.

ACL Audit Analytics technology is used by many leading companies as their primary tool in fighting fraud because it's proven, efficient, and helps find money that is lost to fraud, error and abuse.

ACL technology offers the power to create and run a comprehensive set of tests designed to detect indicators of a wide range of fraud regardless of which IT system houses the transactional data and how many records you need to analyze. With the ability to test 100 percent of transactions, your investigation will uncover all relevant anomalies – typical signs of fraud, error, or abuse. Through automation, these tests run continuously, often catching the fraud early, before the money goes out the door, making remediation easier and acting as an effective deterrent for other potential fraudsters. For more information, visit www.acl.com/fightfraud.