ARIZONA Auditor General
Making a Positive Difference

FRAUD PREVENTION ALERT

Data Analytics: Part 2
October 2018

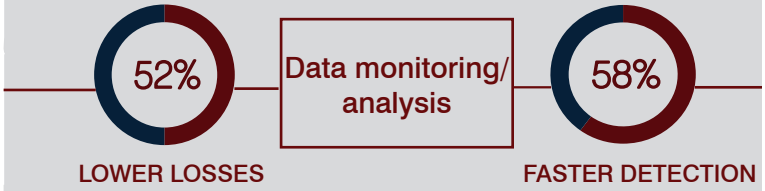
Why are we issuing this alert?

As presented in our November 2017 Fraud Prevention Alert—Data Analytics: Part 1, using risk-based assessments and data analytic techniques to identify trends, patterns, anomalies, and abnormal relationships in data can be an effective anti-fraud control.[1] In fact, data monitoring and analysis techniques have been correlated with the largest reductions in global fraud loss and duration, but only 37 percent of victimized organizations implemented these controls.[2] Data analytic techniques can be separated into three categories for practical applications: basic, statistical, and advanced. This alert, the second in a four-part series, focuses on the practical applications for basic techniques and describes how using these techniques on an organization's data and investigating associated findings can help public officials identify fraudulent activity before it becomes significant.

What are basic data analytic techniques?

Basic data analytic techniques include many methods, such as day-of-the-week validation, vendor-master-file analysis, and classification/summarization, which are briefly described in the textbox on the next page. This alert focuses on the more involved techniques of even-dollar testing, duplicate-payment testing, and gap and sequence validation.

DATA MONITORING/ANALYSIS was correlated with the largest reductions in fraud loss and duration.



Yet only 37% of victimized organizations implemented these controls.[2]

Even-dollar testing

Even-dollar testing procedures can quickly identify transactions of interest for further review. The human tendency to follow a repeatable and predictable pattern remains true for those who perpetrate fraud, and even-dollar testing helps identify some of those predictable patterns. The basic approach for even-dollar testing is to utilize a modulo function (also known as MOD).

This function works by dividing two inputs and evaluating any output remainder. Specifically, divide the first input, a total or subtotal in dollars by the second input, criteria specifically created by the user to meet their needs, such as "10," "25," "100," or "1,000." Take caution when determining this second input because the lower the criteria range, the more results will be yielded, and the less effective the even-dollar test will be. If a lower criteria range is used, consider using sampling techniques to obtain a smaller representative sample of transactions to review. If any reviewed records have an output remainder of zero (meaning that the number is evenly divisible), then it is considered an even-dollar transaction. Each of these even-dollar transactions have a higher risk of fraud and should be investigated to determine propriety.

Duplicate-payment testing

Duplicate-payment testing can isolate payments that may be associated with fraud. For example, when a vendor is paid multiple times for the same services, a duplicated payment can be misappropriated by intercepting the check or altering

---

[1] See Office of the Auditor General, *Fraud Prevention Alert—Data Analytics Part 1*, November 2017, Report 17-406.

[2] See Association of Certified Fraud Examiners, Inc., *Report to the Nations on Occupational Fraud and Abuse*, 2018.

vendor data to have the check delivered directly to the fraudster. The basic approach for detecting duplicate payments is to use a program like ACL (Audit Command Language) to run an exact match test of the population. Common fields for the test are invoice dates, invoice numbers, purchase orders, check numbers, and/or dollar amounts. The more fields that match between two transactions, the higher the risk of a duplicate payment.

Accounting software can and should have settings or controls to prevent duplicate payments; however, the primary purpose of these settings and controls is to prevent duplicate payments generated by mistake. A fraudster can circumvent these controls by transposing invoice numbers, adding numbers to the beginning or end of the invoice number, or using different invoice number conventions (hyphens, slashes, spaces, or special characters). ACL and similar programs can omit these characters by using an exclude or replace function. Using such a function will improve results from the duplicate-payment test and better enable employees to identify transactions that can be further investigated.

Gap and sequence validation

Gap and sequence validation can identify missing transactions. Using sequentially prenumbered documents such as invoices, receipts, and purchase orders is a common and effective control at many entities. A gap in such documents constitutes a missing piece of the audit trail and indicates an increased risk of fraud. The basic approach for gap and sequence validation is to run the GAPS command found in most accounting applications, which will identify sequential variances in an input data set such as receipt numbers, dates, or invoice numbers. Investigate to determine the cause of all variances and gaps identified. If sequential variances, such as gaps in receipt numbers are noted, it could indicate that a receipt was improperly voided or that the receipt was taken.

Additional basic data analytic techniques to consider:

- **Day-of-the-Week Validation:** Detects transactions occurring outside of standard working days. Use a program like ACL to identify unusual transactions that occur outside normal business days or hours.
- **Vendor-Master-File Analysis:** Identifies multiple addresses for one vendor or questionable addresses such as post office boxes. Manually review unusual addresses in order to determine propriety.
- **Classification/Summarization:** Sets expectations for what should happen and compares against what did happen to detect irregularities. Meaningful categories should be created, and data should be organized into those categories to help evaluate reasonableness.

Recommendations

To help protect public monies, public officials should establish proactive data monitoring and analysis programs designed to deter and detect fraud. Specifically, public officials should:

- Review all areas of operation and determine areas that may be susceptible to fraud using a risk-based approach to prioritize the most vulnerable areas.
- Develop and regularly perform data analyses to detect fraud in the identified areas.
- Investigate findings in a timely manner using knowledgeable and trained employees to interpret results.
- Communicate the results to management.