7 Steps to Tackle Fraud Using Data Analytics

DUSTIN LEWIS, CISA
Senior Technical Consultant
ACL Services Ltd.

Contents

As the person given the daunting task of finding fraud within your organization you may be overwhelmed with where to start. Knowing that it's occurring, but not having insight into where, how and by whom – it's like finding a needle in a haystack. While I can't promise the process will be easy – I can tell you that if you follow these 7 Steps using data analytics, you will find that fraudulent activity within your organization, much quicker and more accurately than you would have on your own.

it's like finding a needle in a haystack

Build a profile of potential risks

Fraud risks should be developed as part of an overall risk assessment. You're not likely to make friends throughout the organization by conducting this on your own. If you think it's high time to look into the **fraud potential of purchasing cards**, it's probably a good idea to include the p-card manager in the discussions. That way it's a joint effort that will benefit both parties and hopefully result in a more continuous approach to fraud risks in that area.

You are going to want to focus on risks with the greatest chance of reducing shareholder value, for example:

- Extended supply chain re: safety, quality, reliability of suppliers and processes
- Is there a process to receive and act on regulatory comments or findings?
- Are pricing strategies consistent with regulations and free from collusion?
- Can you detect and avoid discrimination with customers, suppliers and employees?

Plus, by focusing on reducing the risk to shareholders, you make management happy, and this can result in a more robust, long-term fraud program.

Which risks to look at?

With data analysis, you can identify and monitor business risks to ensure you are auditing today's risks, not yesterday's. Consider these:

- Revenue by location, division or product line
- Revenue backlogs – by value and age
- Personnel changes in key positions (legal, controller, R&D)
- Volume of manual JEs or credit notes
- Aging A/R balances or Inventory levels
- Vendor management (# vendors, volume of transactions)
- PCard vs. PO procurement
- Average days for customer payment

Test data for possible indicators

If you are serious about a fraud prevention and detection program, you are **testing 100% of the data, not just random samples**. Use ad hoc testing in addition to more formalized or regular tests. Automate testing to enable:

- Continuous assessment of problem areas
- Scheduled monitoring of other risk areas
- Increased efficiencies within audit

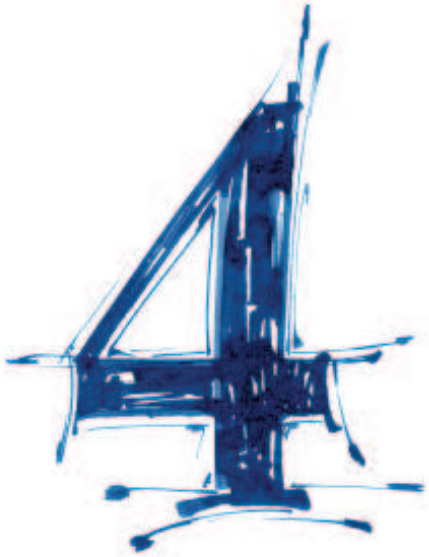
A purpose-built data analytics tool will allow you to access and analyze data from any source internal or external, without compromising data security.

Find out where controls are not working or ineffective. Look for controls that cannot be governed by application control settings. Once you've run some tests, standardize them so they can be used by others and to reduce the impact of staff turnover. What you're doing is creating a repository of analytics that can be used over and over again.

Improve the process by implementing continuous analysis

Run tests on a continuous basis and provide management with immediate notification of a controls breach. Create a process for control remediation to close the loop. This is about building relationships again. By instating a process to deal with issues, you are strengthening your **fraud program** and this can have a huge impact on the way you work with other areas of the business as well as on the bottom line, if cost can be recovered.

Implement continuous auditing/monitoring across business process areas as you grow your program.



Review results

By leveraging and automating technology, you will have more time for the fun part of fraud investigations. Drill down into the patterns and indicators that emerge from your analyses:

- Quantify the risks
- Identify and target high risk areas
- Consider risk monitoring dashboards

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. Automated, scheduled testing will make this simple.

Automated, scheduled testing will make this simple.

Report

As we conclude an investigation, most of us will make recommendations on how to tighten controls or change processes to reduce the likelihood of non-compliance, but how many people are following up on these recommendations? Look into it and find out if the recommended actions have had the desired effect.

Communicate

I recently heard a fraud case study where informal communication was key. The case had to do with a large bottling company that uses fuel cards for its fleet of truck drivers. Last summer, when fuel costs were at their highest, the company reduced costs by $1.4 million. How? In addition to simple tests using both internal and credit card data, word of mouth played a big part. Fraudsters were using the cards during hours they weren't working. A few of them were confronted and the jig was up. Word spread like wildfire and the fraudulent activity ceased pretty quickly once the truck drivers knew their transactions were being monitored, not just tested randomly, but continuously.

Following your investigation, you'll want to communicate your findings, your challenges and successes to management. Schedule a lunch 'n learn session within your organization, make it an agenda item at the next Board meeting, or contribute to the intranet or corporate newsletter.

It can also be professionally rewarding to share your results with your peers by contributing to journals, webinars, and conferences through the ACFE, The IIA and other industry leaders.

Who doesn't love a good fraud story?