ACL WHITEPAPER

Automating Fraud Detection: The Essential Guide

John Verver, CA, CISA, CMC,

Vice President, Product Strategy & Alliances

acl

transforming audit and risk

Contents

Automating Fraud Detection: The Essential Guide

Executive Summary

Data analysis can play a critical role in identifying indicators of fraud in most business process areas. By implementing risk and control data analytics to regularly monitor business transactions—and integrating them into an overall risk and control process—management can identify and respond quickly to red flags, and reduce the risk of fraud escalation. Through a discussion of typical frauds, detection processes and tests, you will learn how to achieve results by applying data analysis software in key business areas.

Introduction

During the past five or so years, surveys of senior professionals in the areas audit, risk management, compliance, and fraud detection have consistently shown that increased use of technology is considered to be a critical factor for successful performance. More specifically, the surveys have found that data analysis software is the technology that is expected to have the greatest impact on effectiveness and productivity.

So, how, in practice, can data analysis software be used to improve and automate fraud detection processes and support overall risk management? This paper identifies some of the key issues in implementing a fraud detection program and provides examples of fraud detection tests for common business process areas.

Integrating Fraud Detection through Audit, Risk Management, and Compliance

One of the first issues to consider in implementing a fraud detection program is more of a strategic one: Ownership. Is the organizational objective to integrate fraud detection analytical testing processes into those of overall risk management and control, or is it instead to perform them within a standalone function? The specific technical use of data analysis will not vary much in either case, but the people and process aspects will usually require different considerations.

Data analysis, often in the form of continuous monitoring of transactions and controls, is increasingly used as a key component of risk management and audit processes overall. For many organizations it makes sense to integrate fraud detection objectives into risk management and audit processes, since the risk of fraud is simply one among many risks that an organization faces and should be considered within the full spectrum of risks. In other organizations, there may be a more specific functional area focus on fraud, which necessitates different considerations be given to the practical aspects of implementing data analysis approaches.

The Role of Data Analysis in Fraud Detection

The fundamentals of using data analysis to detect fraud are reasonably simple.

The objective is to analyze entire populations of transactional data (as well as, perhaps, master data and application control settings) in order to look for indicators of fraudulent activities. Reliance on examination of only a sample of data is insufficient for finding warning patterns, and also often inadequate to fulfill regulatory needs.

Types of data analyses may vary. For example, techniques can range from statistical analysis designed to look for transactions outside the norm of what is expected, through to analytic tests that look for specific circumstances that indicate a high probability of fraud. Statistical analysis produces summary reports and allows drilldown into exceptions. The second type of testing is specific, for example, a test designed to identify matches between employees and suppliers.

Fraudsters often take advantage of the gaps between business systems, which typically don't exchange information. One of the most effective analysis techniques can be to compare data across different databases and systems—often in ways that are never

[1] *PricewaterhouseCoopers, State of the Internal Audit Profession Study (2008-2013)*

normally compared. A simple example would be to examine all supplier payment transactions for instances in which a supplier name, address, or bank account is the same as an employee. One way to uncover this is to test specific database fields from, for example, an SAP ERP system in comparison with human resources records in a PeopleSoft system, using "fuzzy" matching logic to identify close variations on the spelling of names and address combinations.

Some types of analytic procedures can appear superficially simple, such as looking for duplicate payments of an invoice made fraudulently by an employee in collusion with a vendor. In practice, however, these seemingly simple procedures may require sophisticated design in order to avoid the issue of false positives, particularly if the tests are to be performed on an ongoing automated basis.

One of the biggest potential drawbacks to the use of data analytics arises when a test creates excessive numbers of exceptions for investigation. An important consideration in building a fraud detection program is to avoid this obstacle by ensuring that analytic tests take account of anomalies that are known not to be fraudulent—with evolving intelligence over time. In working practice, the fewer exceptions that arise and the higher the probability that they actually indicate fraud, the more likely that the results of testing will be actively investigated.

What to Look For: Capabilities of Data Analysis Software for Fraud Detection

Most data analysis software designed specifically for audit, fraud detection, and control testing have similar functional capabilities. They usually include pre-built analytic routines, such as classification, stratification, duplicate testing, aging, join, match, compare, as well as various forms of statistical analysis. The more powerful ones include a high degree of flexibility to support full automation and the development of complex tests that address the sophistication of some fraud detection requirements.

One important capability to look for in data analysis software for audit and fraud detection is that of logging of all procedures performed. This can prove to be of importance in generating complete audit trails that may be required to support detailed investigation and subsequent prosecution.

Whether for fraud detection purposes or other audit and control testing purposes, there are important advantages to analyzing data independently of an organization's application systems themselves. Data analysis technology addresses the control gaps that often exist within enterprise resource planning (ERP) systems. While ERP systems may have certain capabilities to prevent or detect fraud and errors, or to flag exceptions, most fraud professionals find that they not are sufficient to effectively trap the typical problem transactions that occur. For example, in many cases, certain control settings are turned off to enable the ERP system to run more efficiently. Additionally, while Business Intelligence (BI) tools are good for providing summary level information or high-level trends, they are not as effective in performing detailed testing. Performing independent data analysis allows you to critically examine individual transactional details, which better enables identification of fraud and abuse.

In practice, another of the most important capabilities of data analysis technologies for fraud detection is the ability to access a broad range of data. As mentioned, there may be a requirement to compare data from a range of data sources, both internal and external. The technical structure of data from different sources may vary considerably. Specialized fraud and control testing software should include the ability to access and combine data in ways that are not commonly available in more general purpose analysis software or from standard ERP system reports.

Program management and remediation workflow can also play a helpful role in managing a fraud program, so stakeholders can stay on top of program activities and issues remediation. Additionally, in organizations where fraud detection is integrated into an overall risk management process, capabilities to manage an overall risk assessment process and deliver dashboard reporting become critical in order to provide ongoing insight into strategic risks—including fraud—for executives.

Automation of Fraud Detection Analytics and Continuous Monitoring

Once a particular test has been developed in order to detect a specific fraud indicator, it will often make sense to repeat the analysis on a regular basis against the most recent transactions. There are obvious advantages in detecting fraud sooner rather than later, before the extent of fraud has escalated. According to the Association of Certified Fraud Examiners' most recent *Report to the Nations on Occupational Fraud and Abuse*, the typical fraud case continues for 18 months before it is detected. Timely risk mitigation often makes a strong business case for analyzing and testing transactions on an ongoing basis.

The frequency of this form of continuous monitoring will vary depending on the nature of the underlying process. For example, in the case of monitoring payment and revenue transactions, it may make sense to perform automated testing on a daily basis. For areas such as procurement cards or purchase cards (P-Cards), travel and entertainment (T&E) expenses, and payroll, testing is more typically performed on a monthly or weekly basis in correlation with payment frequencies.

From a technical perspective, the progression from using a suite of fraud specific data analytics on an ad hoc basis to that of continuous monitoring is not particularly complex. Assuming the issues of data access, preparation, and validation have been addressed—and that the tests have been proven to be effective—the move to continuous monitoring simply involves the regular automation of test processing. The important issues to address are those of people and process. For example: Who is responsible for reviewing and following up on the results of testing? How often is the review and follow up to take place? How are unresolved items addressed? Who is responsible for the decision to initiate in-depth investigation and interviews? Etc.

Software designed for continuous monitoring supports this process by providing a workflow for remediation. This means that exceptions generated by specific tests are automatically routed to specific individuals for review. Notification of high risk exception items may be also routed to more senior management.

Continuous monitoring fraud detection software should also provide dashboards that visually summarize the results of analysis and test processing over a period of time. This allows senior management to review trends in the nature and amount of exceptions identified, as well as the status of items that are unresolved or under investigation. This form of reporting should ideally be integrated into an overall "data-driven" risk management dashboard that provides timely, visual representation of fact-based insight excavated from business transaction data.

Example Fraud Tests For Key Business Process Areas

Most organizations begin automated fraud detection in either the common business process areas (e.g., Purchase to Pay, Payroll, Order to Cash, Travel and Entertainment) or areas that are industry specific and particularly high risk (e.g., insurance claims, banking loans, healthcare billing, retail point-of-sale (POS), telecommunications billing).

It is usually most effective to start with a core set of relatively straightforward tests and progressively build and implement a broader "library" of tests for different business process areas.

In practice, organizations may develop large libraries of tests over time. The fraud specialist or auditor is often in the best position to understand a specific fraud risk given the underlying business process. Analytics should ideally be developed to reflect both known risks as well as to create reports that indicate potential risks in circumstances that are not likely to be foreseen.

The following are examples of some common data analysis tests performed in standard business process areas.

Purchase to Pay (P2P)

- P.O. with blank / zero amount
- Split P.O.s (multiple under approval threshold)
- Duplicate invoices (same #, same amount on same date, same vendor with same amount)
- Invoice amount paid > goods received
- Invoices with no matching receiving report
- Multiple invoices for same P.O. and date
- Pattern of sequential invoices from a vendor
- Non-approved vendors
- Suspect purchases of consumer items
- Employee and vendor with same:
  - Name
  - Address
  - Phone number
  - Bank account number
- Vendor address is a mail drop
- Payment without invoice
- Vendor master – changes for brief periods

Purchasing cards (P-Cards)

- Purchases of consumer items
- Suspect vendors
- Prohibited merchant codes
- Transactions made on weekends or holidays
- Split transactions (multiple items under threshold)
- Duplicate purchases (same item multiple employees)

Order to Cash (O2C)

- Unusually high sales discounts
- Unusually high credit terms/credit limits
- Frequent credit memos to the same customer
- Shipments where employee address matches the ship address

Payroll / HR

- Terminated employees still on payroll
- Multiple employees with same address
- Unusually high O/T amounts and rates
- Invalid SSNs
- Unusually high commissions

Additional information on fraud tests by business process and industry is available on www.acl.com/fraud

Getting Started

Data analysis can play a critical role in identifying fraud risk indicators. To get started, here are the basic steps that typically need to be addressed in order to create an effective and sustainable automated fraud detection process.

How to get started

Practical steps for implementation of data analysis technology for fraud detection

1. **Define overall objectives,** particularly in terms of whether the fraud detection process is part of an overall risk management and control testing strategy or a standalone function.
2. **Assign initial responsibilities** for each of "people, process, and technology," both for the implementation project and ongoing fraud detection.
3. **Identify and define the specific fraud risks to be tested**—effectively creating a "fraud risk universe."
4. **For each risk, identify and define** a data analysis fraud detection test in terms of:
   - data requirements
   - data access processes
   - analysis logic
5. **Coordinate with IT department** as needed for issues of data access and any centralized processing requirements.
6. **Develop the tests.**
7. **Validate the effectiveness** of the tests.
8. **Establish timing and responsibilities** for automated test processing.
9. **Establish workflow and responsibilities** for exception management and resolution.
10. **Implement reporting processes.**

By implementing risk and control data analytics to regularly monitor business transactions, management can identify and respond quickly to red flags, and reduce the risk of fraud escalation—as well as support overall risk management and control processes.

John Verver, CA, CMC, CISA, is Vice President of Product Strategy & Alliances at ACL. He is a long-time proponent of the use of technology in audit, risk management, internal control, and fraud detection. He is a Chartered Accountant, Certified Information Systems Auditor, and Certified Management Consultant. He was a key contributor to the IIA's Global Technology Audit Guide #3 on Continuous Auditing and is on the advisory board of the Continuous Audit Research Lab at Rutgers University. Prior to joining ACL, John spent 15 years with Deloitte in the UK and Canada, with responsibility for IT audit and security services, as well as accounting systems consulting and implementation, and subsequently becoming a principal.

About ACL

ACL delivers technology solutions that are transforming audit and risk management. Through a combination of software and expert content, ACL enables powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

Driven by a desire to expand the horizons of audit and risk management so they can deliver greater strategic business value, we develop and advocate technology that strengthens results, simplifies adoption, and improves usability. ACL's integrated family of products—including our cloud-based governance, risk management and compliance (GRC) solution and flagship data analytics products—combine all vital components of audit and risk, and are used seamlessly at all levels of the organization, from the C-suite to front line audit and risk professionals and the business managers they interface with. Enhanced reporting and dashboards provide transparency and business context that allows organizations to focus on what matters.

And, thanks to 25 years of experience and our consultative approach, we ensure fast, effective implementation, so customers realize concrete business results fast at low risk. Our actively engaged community of more than 14,000 customers around the globe—including 89% of the Fortune 500—tells our story best. Here are just a few.

Visit us online at www.acl.com

acl
transforming audit and risk