USING TECHNOLOGY TO AUTOMATE FRAUD DETECTION WITHIN KEY BUSINESS PROCESS AREAS

Technology can play a critical role in identifying indicators of fraud in most business process areas. By implementing suites of analytic tests that regularly monitor transactions, management can respond quickly to red flags and reduce the risk of fraud escalation. Through a discussion of typical frauds, symptoms, and tests, you will learn how organizations have seen immediate results through the use of audit analytics technology in key business areas.

JOHN VERVER CA, CISA, CMC
Vice President, Product Strategy & Alliances
ACL Services Ltd.
Vancouver, BC

John Verver, Vice President, Product Strategy & Alliances, has overall responsibility for ACL's product and services strategy, as well as for relationships with key organizations in the audit and control market. Verver is acknowledged as an expert and domain thought leader on continuous controls monitoring and analytics for audit, risk management, and compliance. He is regularly asked to speak at global audit and control conferences and is an inaugural member of the Center for Continuous Auditing's advisory board. Verver was a key contributor to the Institute of Internal Auditor's Global Technology Audit Guide #3 on continuous auditing and controls monitoring. Prior to joining ACL more than 20 years ago, Verver spent 15 years with Deloitte in the UK and Canada where he was a principal and Director of Computer Services with responsibility for IT audit and security services, as well as accounting systems consulting and implementation. Verver is a Chartered Accountant, Certified Management Consultant, and Certified Information System Auditor.

ACFE™
Association of Certified Fraud Examiners

NOTES

Introduction

During the past 5 or more years, surveys of senior professionals in the areas of 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 is the technology expected to have the greatest impact on effectiveness and productivity.

So, in practice, how can data analysis technologies be used to improve and automate fraud detection processes? This paper identifies some of the key issues and provides examples of fraud detection tests for common business process areas.

Fraud Detection and Integrated Audit, Risk Management and Compliance

One of the first issues to consider is more of a strategic one. Is the organizational objective to integrate fraud detection analytical testing processes into those of overall risk management and control or to perform them within a stand-alone function? The specific technical use of data analysis will not vary much in either case, but the people and process aspects will usually be different. 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 these processes as the risk of fraud is simply one of the many risks that an organization faces and should be considered alongside the full spectrum of risks. In other organizations, there may be a more specific functional focus on fraud which means that different considerations must be given to the practical aspects of implementing data analysis approaches.

NOTES

Role of Data Analysis Technology in Fraud Detection

The fundamentals of using data analysis technology 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. The types of analysis may vary from statistical analysis designed to look for anomalies that could indicate a possible fraud, through to analytic tests that look for specific circumstances that indicate a high probability of fraud.

One of the most effective analysis techniques can be to compare data across different databases and systems—often in ways that are never normally compared. A simple example is to test all supplier payment transactions to see if there are instances in which the supplier name or address or bank account is the same as an employee. This could involve testing specific data base fields from, say, an SAP ERP system and comparing it to a PeopleSoft HR 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—e.g. looking for duplicate payments of an invoice made fraudulently by an employee in collusion with a vendor. In practice they may require to be designed in a more sophisticated way 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. The objective is to avoid this situation by ensuring that analytic tests take account of anomalies that are known not to be fraudulent. In practice, the fewer exceptions that arise and the higher the probability that they actually indicate

NOTES

fraud, the more likely that the results of testing will be actively investigated.

Capabilities of Data Analysis Technologies for Fraud Detection

Most data analysis technologies 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.

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 indicated above, 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.

NOTES

Automation of Fraud Detection Analytics and Continuous Monitoring

Once a particular form of analysis has been produced in order to detect a specific fraud indicator, it will often make sense to repeat the process 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. So there is often a good business case for analyzing and testing transactions on an ongoing basis. The actual timing of this form of continuous monitoring will vary depending on the nature of the underlying process. In the case of monitoring of payment and revenue transactions it may make sense to perform automated testing on a daily basis. For areas such as procurement cards, travel and entertainment expenses and payroll, testing is more typically performed on a monthly or weekly basis.

From a technical perspective, the progression from using a suite of fraud specific data analysis tests 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, then 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? Software designed for continuous monitoring supports this process by providing workflow capabilities. 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

NOTES

management. Continuous monitoring fraud detection software should also provide dashboards that 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.

Practical Steps for Implementation of Data Analysis Technology for Fraud Detection

The following are the basic steps that typically need to be addressed in order to create an effective and sustainable automated fraud detection process:

- ❑ 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 stand-alone function.
- ❑ Assign initial responsibilities for “people, process, and technology,” both for the implementation project and ongoing.
- ❑ Identify and define the specific fraud risks to be tested—effectively creating a “fraud risk universe.”
- ❑ For each risk, identify and define a data analysis fraud detection test in terms of:
  1. data requirements
  2. data access processes
  3. analysis logic
- ❑ Coordinate with IT departments as needed for issues of data access and any centralized processing requirements.
- ❑ Develop the tests.
- ❑ Validate the effectiveness of the tests.
- ❑ Establish timing and responsibilities for automated test processing.

NOTES

- ❑ Establish workflow and responsibilities for exception management and resolution.
- ❑ Implement reporting processes.

Examples of 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, T&E) or areas that are industry specific and particularly high risk (e.g. insurance claims, banking loans, healthcare billing, retail POS, telcom billing).

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

The following are just examples of some common data analysis tests performed in each common business process area. In practice, organizations may establish large libraries of tests over a period of 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.

Purchase to Pay

- ❑ P.O. with blank/zero amount
- ❑ Split P.O.’s (multiple under approval threshold)
- ❑ Duplicate invoices (same #, same amount same date, same vendor 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

Procurement 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

- ❑ 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

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

NOTES