WHITE PAPER

The ACL Audit Analytic Capability Model:

Leveraging analytics in the fight against fraud

CONTENTS

"The ACL Audit Analytic Capability Model provides the kind of practical guidance many organizations are looking for today. The audit profession understands the value of analytic technology but thus far has lacked a clear roadmap that outlined the steps required to integrate it into their audit processes. This model helps do that, addressing not only the technology but also the people and processes that are critical to success."

Dave Coderre,
President of CAATS, & leading author
(*"Computer-Aided Fraud Detection & Prevention: A Step-by-Step Guide"*)

INTRODUCTION

Today's business climate has heightened overall awareness of occupational fraud and abuse and its impact on organizations of all types and sizes. It has also increased management's expectations of fraud examiners and other assurance providers to be more vigilant and more proactive in the early identification – if not prevention – of fraud. Not only are assurance providers being asked to become more efficient and effective in performing this critical role but expectations are heightened to also assess the risk of fraud in their organizations – a challenge that is amplified by declining or, at best, flat budgets, increasing complexities around regulatory compliance and fewer staff.

For more than 20 years, ACL Services, Ltd. has worked closely with more than 14,700 customer organizations worldwide to develop audit analytic solutions to assist fraud examiners and assurance professionals to leverage the power of data in providing higher levels of insight into their organization's business activities. During this time, ACL collected in-depth intelligence from customers who have benefited from using audit analytics, as well as valuable evidence from those who have not.

Based on this knowledge, the Analytic Capability Model was developed as a framework for assessing different levels of analytic techniques and associated benefits. The model illustrates five progressive levels through which fraud examiners should be looking to evolve their use of analytics, and outlines the fundamental building blocks, in terms of people, process and technology that must be in place to optimize benefits.

This model was developed to help organizations more clearly evaluate their use of analytics and to better understand, plan and communicate what needs to be done to achieve and increase benefits and success in fraud detection and prevention. This paper provides an introduction to the Analytic Capability Model and help organizations build a roadmap for increasing analytics testing throughout their fraud detection activities.

THE ANALYTIC CAPABILITY MODEL

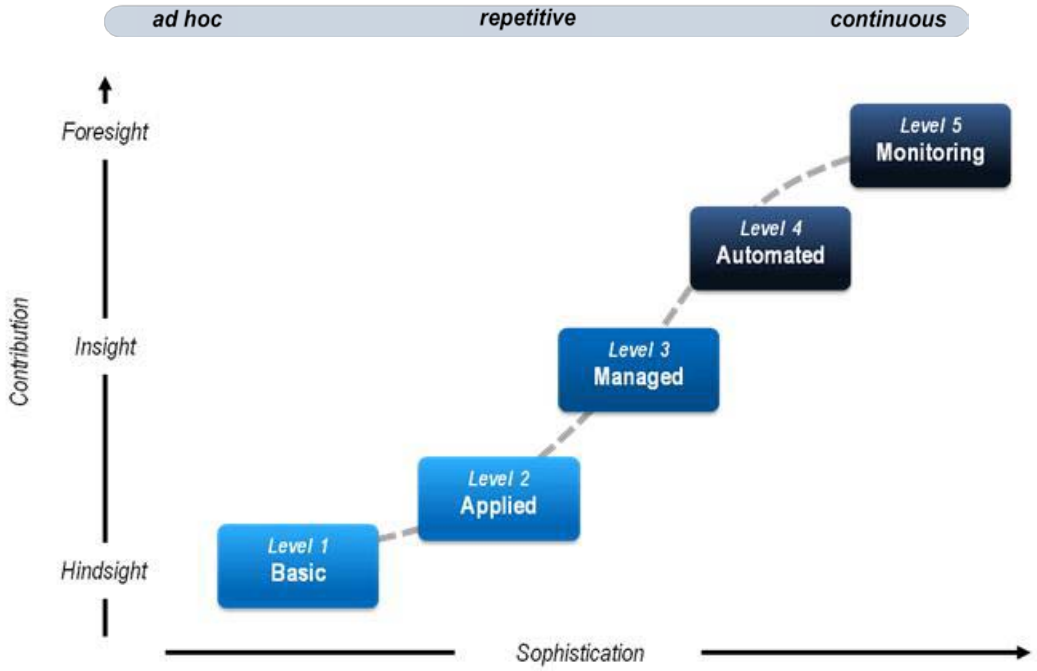
The traditional approach to fraud detection has often been to take a historic or retrospective view of what has happened over a long period of time. While this approach delivers necessary and proven hindsight in terms of what has happened, today's environment demands a more proactive and comprehensive approach for fraud detection and prevention.

The Analytic Capability Model illustrates five levels through which fraud examiners can expand the use of data analytics to increase benefits: Basic, Applied, Managed, Automated and Monitoring.

For most organizations, the sophistication of analysis capabilities correlates with the value and contribution that fraud examiners can deliver to the business by analyzing data. As a fraud detection program extends its use of analytics, it can evolve into a fraud prevention program based on automation and continuous analysis of business transactions. This enables fraud examiners to shift from a reactive reliance on whistle-blowers or tips to a more proactive approach for identifying fraud and managing the risk of fraud, and delivers hindsight, insight and foresight for greater value to the business. (See Figure 1.)

"This enables internal audit to shift from a reactive to a proactive approach for identifying and managing risk, and delivers hindsight, insight and foresight for greater assurance and value to the business."

Figure 1: ACL's Audit Analytic Capability Model



Data analysis by fraud examiners plays an important role at each stage of the continuum. For example, analytics can be used to support specific fraud investigations and to test 100% of transactions over the period in question, or from one year or previous quarter. This enables fraud examiners to identify where control failures have occurred in the past, delivering essential hindsight for compliance, governance and risk management.

As investigations expand the use of analytics as a centrally managed tool that is integrated into fraud detection and prevention processes, data analysis provides more timely insight into risks and controls at a level that is simply not possible without technology. Testing procedures can be repeated to enable timely analysis of large data sets and to identify detailed instances of risk, fraud and abuse across multiple business process areas.

As organizations apply greater automation and continuous fraud detection and monitoring for fraud, analytics provide the ability to detect patterns or trends and control issues that provide foresight on increasing or changing fraud risk within business and financial control processes. For example, controls monitoring routines can be run on a daily basis. Regular analytic tests can reveal instances of specific transactions that are a threat, as well as opportunities for improving controls to prevent fraud from occurring to begin with.

Improving fraud examiners line of sight is enabled by a progression towards continuous analysis and monitoring. Many organizations understand the benefits of automated continuous fraud detection and monitoring and want to move there immediately. However, without the building blocks of the lower levels in place, in terms of people, process and technology, it is more difficult to achieve the intended benefits.

This Analytic Capability Model is intended to help organizations evaluate their use of analytics as they progress through the levels.

"Uncovering and stopping this fraud, in addition to recovering millions in lost tax revenue on behalf of the Ministry, was made possible by using ACL technology. In addition, because of the new audit standards for all EU member countries, the Austrian Ministry of Finance is using ACL analytics for ongoing monitoring and auditing."

Bernhard Kurz, Senior EDP Auditor
Austrian Ministry of Finance

In the next section, we will explore the characteristics and benefits of each level. Additionally, we will look at some of the challenges that fraud examiners face while using analytic technology, as well as the risks that organizations may face at each level. We will also provide tips on how to optimize people, processes and technology to reduce those risks and improve the effectiveness of fraud detection analytics as organizations expand their use from data analysis toward continuous monitoring.

LEVEL 1 - BASIC

Organizations performing at the Basic level use data analysis technology to perform ad hoc queries and analysis of large data sets, most often for specific fraud investigations. Analytics could be used in a forensic context, seeking out the evidence of a fraud already identified, with a view to gathering evidence for prosecution. Alternatively, analytics could also be used by fraud examiners to seek out indicators of fraudulent activity in the organization's data, with the objective of proactively detecting fraud. In this scenario, the user typically starts by using analytics to produce statistical overviews and classifications or summarizations of data. This allows the examiner to identify anomalies and to better understand the transactions and balances within a specific area. Obvious problems such as duplicates are easily identified with pre-built analytic tests. Transactions and master data can be compared between systems, providing indicators of errors and fraud, such as matches between employee information and vendor details.

Characteristics

At the Basic level, the use of data analytics is typically ad hoc and undertaken by those who have received introductory training. There is usually little involvement from management. Often a user with technical interests selects the analytic software, which is then used by that individual or only a limited number of specialists within the broader fraud detection team. As a result, the individual or a small team of data analysts often become skillful power users who are highly productive in terms of output.

Benefits

With initial use of audit analytic software, users rapidly gain a better view of risk and control issues within a given business area. Analysis is more in-depth than can typically be obtained by general-purpose software or by manual procedures alone. For example, audit analytics allow for the review of 100% of transactions or balances and the use of pre-built queries designed for investigative purposes.

As a result, users can quickly identify specific instances of fraud and abuse, as well as control weaknesses that could be exploited by fraudsters. In some cases, the time to analyze data can be cut down from days to minutes when compared to manual techniques.

Challenges

The most common challenge for those just starting to implement analytics at the Basic level relates to data access. This includes understanding what data is required to support a specific fraud test and getting a complete and controlled population of that data.

Organizational Risks

Just as data access issues may challenge the fraud examiner at this level, obtaining data can become a significant risk and resource constraint to the organization if the process is not planned and managed effectively.

Because audit analytic software can handle massive amounts of data, security is paramount. For example, an organization would not want an entire payroll or payment run to wind up on a laptop or network server with inadequate security.

There is also risk that an investigator may jump to conclusions based on analysis that has not been thoroughly understood. It is important to realize that analytics may point out possible indicators of fraud – not prove that a fraud has been committed. Analytics will help the professional fraud investigator focus in on the suspect transactions. Formal, certified training in the use of analytics and in investigative procedures is critical in this situation.

How to Optimize

By focusing on improvements in the areas of people, process and technology, organizations can overcome these challenges and risks and increase the effectiveness of analytics at the Basic level:

People

- Train your team. Although data analysis software is not difficult to use at a Basic level, training is important and beneficial.
- Unless the IT department is mandated to support the fraud investigator, it is often a good idea to have a strong technical resource available that can help deal with arranging access to data.

Process

- Start with a simple plan. Identify where to use data analysis, the fraud detection/investigation objectives that are supported, the period to be covered and the timeframe in which the work will be performed.
- Work with the IT department to identify and gain access to appropriate data.
- Ensure that the data obtained is actually the desired data and is complete.
- Determine the nature of reports and documentation of procedures performed.

Technology

- Select analytic software that is not only effective at the introductory level but that can also support continuous fraud detection and monitoring for future growth.
- Ensure hardware systems can support large volume data storage and processing.
- Leverage your software's built-in logging capabilities to create a body of evidence that records the analytics performed during the investigation.

LEVEL 2 – APPLIED

The second level builds upon the first, but is distinct in that the analytics are far more comprehensive, are fully integrated into the detection process and begin to transform how fraud investigations are performed.

At this level, fraud detection planning and program design takes analytics into account, effectively creating an "analytic-enabled fraud detection program." In such a program, wherever beneficial and practical, a fraud objective is achieved with the help of a specific analytic test.

Characteristics

Within this level there is a broad range of skills and applications. People and process issues become increasingly important at this level. Management needs to provide direction and support, and a specialist is often assigned the role of data analyst to oversee the development of analytic projects and procedures. Review and quality assurance procedures are put in place to confirm the quality and validity of the detective analytics that are performed.

The use of analytics is progressive within this level. After starting with "low-hanging fruit," usage grows over time as additional tests are added to support a broader set of fraud detection objectives. Consideration is given to how analytics can best be applied on every new investigation.

Additionally, training becomes in-depth and technical, with a focus on data access and integration and efficient script design for repeatability. For the manager, training in how to effectively oversee and leverage the analytic process becomes invaluable for integrating the benefits of analytics throughout the detective function.

Benefits

At this stage, analytics begin to fundamentally transform the investigative process, providing substantial improvements in efficiency and greater levels of assurance. Manual analysis, sampling and testing procedures are reduced to those situations requiring physical verification. As a result, many tasks are performed in a fraction of the time, freeing up time for fraud examiners to investigate identified indicators of fraud in the data and to assess areas where control weaknesses have been identified.

Challenges

There are a range of challenges that the team may face as it adopts widespread implementation of analytics and integration into the fraud detection process.

For instance, users must recognize that there is a big difference between the occasional use of an analytic tool and making analytics a core part of the fraud detection process. Analytic programs need to be owned, processes changed, roles changed and people trained, all of which takes time, effort and resources. The payback can be considerable, but cannot be achieved without up-front investment.

In addition, many of the same data access challenges associated with the Basic level also exist at the Applied level. However, as organizations evolve their use of data analytics and implement repeatable tests, these issues need to be integrated into formal test design and development processes, with appropriate quality assurance (QA) procedures. Attention must also be given to documentation standards so tests can be maintained and understood by others.

Organizational Risks

At this level, the greatest risks to an organization are often a result of the decentralized and distributed environment that evolves from the expanded number of end users and increasing analytic content.

As the data environment shifts to a more distributed and decentralized one, the risk of inefficient duplication of effort across different locations increases. Data and tests tend to proliferate across individual laptops, desktops and network servers, making it difficult to manage and keep track of current and correct versions, as well as any subsequent results.

Security issues also increase as data and results proliferate across a range of laptop and desktop computers. Critical data on personal computers may not be subject to the usual enterprise security standards. Particularly sensitive data, such as credit card and social security numbers and investigative findings, is often not encrypted and may be visible to onlookers.

Complex processing of large volumes of data can consume all the processing power of laptops, desktop and network servers for considerable periods of time.

Lastly, there is a good chance that knowledge rests in the heads of a few key individuals whose possible departures could cause a loss of investment and progress.

How to Optimize

To overcome these challenges and risks and to maximize the effectiveness of audit analytics at the Applied level, organizations should consider the following:

People

- Assign overall responsibility for the success of an analytics-enabled fraud detection program to someone with technical skills. However, fraud management should remain closely involved in reviewing objectives and progress.
- Develop and train specialists in data access and test development.
- Keep in mind the need to merge technical and fraud examiner expertise when determining leadership roles. Few fraud examiners are able to successfully combine capabilities in technical data analysis with in-depth understanding of detective and control processes and objectives without appropriate training.
- Ensure management review of test logic and results. Too often, analytics are left to specialists to design with minimal review at a management level.

Process

- Define and broadly communicate goals and objectives for using analytics and establish a realistic estimate of resource and investment requirements.
- Develop a comprehensive analytics-enabled fraud detection program plan that can evolve to meet the needs of subsequent Analytic Capability Model stages. Start with key audit objectives and determine which can be achieved most efficiently and effectively through the use of data analysis.
- Develop procedures for quality control of analytics development and use, such as independent review to ensure that test logic is correct.

Technology

- If data access challenges exist, consider specialized data connectors, for example, to ERP systems or other core business applications.

LEVEL 3 – MANAGED

The Managed level is a logical evolution from the comprehensive use of audit analytic tests as a core part of the fraud detection process. The objective at this level is to achieve team-based data analysis in which data and processing is centralized, secure, controlled and efficient.

Organizations operating at the Managed level must have the people, processes and technology in place to effectively manage the content and activities. Functioning proficiently at the Managed level is also a crucial building block for getting to the next levels in the model.

Characteristics

The Managed level typically involves the development of many analytic tests that process large volumes of different data sets and generate results that often involve confidential information. In most cases, many people are involved in this process and information is spread across various computers in multiple and often geographically diverse locations.

Organizations performing at this level typically have a well-structured and centrally-managed server environment to store and maintain the large data sets and content of the analytic processes (e.g., tests, results, evidence, documentation and related materials).

Complex processing of large data volumes is typically performed on high-powered servers. Access to and use of content is subject to planned processes and is controlled and secure. Procedures, standards and documentation for audit analytics are even more formal than at the Applied level.

Most significantly, at this level it is more practical and common for non-technical staff to efficiently access and use the results of tests.

Benefits

There are numerous benefits to moving to the Managed level of analytics. Team efficiency is greatly improved as it becomes easier and more efficient to share analytic content amongst the entire team, not just analytic specialists.

At this level, analytic work is easily repeatable and sustainable. There is less dependence upon any one individual and therefore less risk of existing work becoming unusable because a team member has left.

A centrally-managed repository also supports processes that make it easier to maintain the quality and integrity of fraud detection analytics and investigative results. Access and changes to tests can be controlled more efficiently and enterprise-level data security standards can be easily maintained. A centralized analytics system is based on a server, which means that processing performance typically improves and less time is spent accessing large data sets and waiting for large and complex analytics to complete.

Establishment of a server-based repository can be an opportunity to improve effective relationships with IT by adhering to more typical standards for storing and processing data, an approach that usually gains the support of IT.

Additionally, it is far easier for management to obtain an overview of all work being performed and to review tests and results since all necessary information resides in one location.

Challenges

Moving to a managed analytics model requires preparation. Establishing a managed and centralized environment for fraud detection analytics is as much about process and people as it is about technology. This means that implementation needs planning, preparation and resource allocations. The time and other resources required to properly plan and implement can be significant, but typically deliver quick return on investment when ongoing growth and scalability can be supported with minimal extra effort or re-work.

Organizational Risks

Other than implementation challenges, there are few immediate risks to an organization that has evolved to a managed environment for analytics. The issue is more one of senior executive expectations for moving to continuous procedures. At this point, the fraud detection team has typically built a suite of tests and implemented procedures to maximize benefits from analytics in support of a cyclical fraud detection process. The tendency can be to assume that everything is in place to start continuous fraud detection.

Although the basic building blocks for continuous fraud detection may be in place, effective continuous analysis requires additional planning and implementation support, particularly from a people and process perspective.

How to Optimize

The following are a few areas an organization should consider for improving the effectiveness of analytics at the Managed level.

People

- Implementation of the Managed level of analytics is as important and integral a component of the overall process as at Level 2. It requires overall leadership and direction by management.
- Designate a repository administrator. The role of repository administrator is an important one. The individual does not have to be a technical specialist, but does need to understand the organization and processes and how to establish effective content security procedures.

Process

- Structure the analytics repository so that content can be used and controlled efficiently. For example, categorize data by fraud area, location and period.
- Carefully consider account access, security and control requirements. Limit access to sensitive payroll and payments data, and prevent changes to tests except by authorized individuals.
- Determine which data is to be maintained in the repository, as well as the timing of data refreshes. Encrypt or mask sensitive data.
- Confirm the completeness and validity of repository data, for example by reconciliation to control data or to general ledger balances or vendor master files.
- Standardize localization and structure of documentation for data, tests and procedures.

Technology

- Ensure software is designed to manage and control analytics content and support efficient access to and refresh of data.

- Ensure server hardware is in place to support a centralized analytics server.

LEVEL 4 - AUTOMATED

Once a comprehensive suite of tests is developed and well managed, your fraud detection approach is ready to move ahead with automation. At Level 4, much is already in place from a technology perspective to begin continuous fraud detection. However, to be effective, continuous fraud detection using analytics involves some fundamental changes in processes.

A continuous fraud detection methodology is different in that the processes for running tests, reviewing and reporting on results are ongoing. Roles and responsibilities for performing continuous analysis are different than for a more traditional investigative approach.

Characteristics

The Automated level builds upon the previous levels as the foundation for continuous monitoring. Comprehensive suites of tests have been developed, tested and are available in a central, controlled environment. Data access for analysis and tests is secure but easily accessible by stakeholders. All that remains from a technology perspective is to schedule tests to run regularly against appropriate period data.

However, continuous analysis requires more than technology issues to be addressed. It usually requires a significant shift in processes. Most departments commence continuous analysis in one area and then expand to additional areas over time as appropriate procedures are established. Automated analytics make it possible to perform concurrent, ongoing fraud detection of multiple areas.

Benefits

Shifting from a historic assurance process to one that is current meets the increasing expectations from management for greater insight and assurance that is timely and subsequently of far higher value.

Once a high level of automation has been achieved, the ability to track current status of fraud risk and control issues leads to a more efficient and effective process overall. Users and management alike can keep track of changes in risk profiles and focus efforts as needed.

For business process areas that show little or no significant issues, continuous fraud detection procedures can save considerable expense and effort. Your resources can be assigned to areas of more significant risks, such as in new business areas and in areas where analytic procedures are not yet in place.

Challenges

A successful move from traditional processes is difficult to achieve unless it is led and supported by senior management who not only understand the benefits and objectives, but also the investment and effort required.

There can certainly be technical challenges in moving to continuous fraud detection – from both audit and technology perspectives – but the more significant challenges are usually encountered when allocating sufficient resources to support the change in approach, as well as recognizing that change of this type requires ongoing review and involvement.

Organizational Risks

Effective continuous fraud detection can provide clear benefits in terms of productivity and effectiveness. However, the greatest risk to an organization is that findings are not responded to in a manner that results in appropriate remedial action and that adds value to the business through improved controls risk mitigation

How to Optimize

Below are a few areas an organization should consider when looking to improve the effectiveness of fraud detection analytics at the Automated level:

People

- Designate a continuous fraud detection program manager who is responsible for leading and coordinating efforts across people, process and technology.
- Modify work processes so that an individual's continuous fraud detection responsibilities other fit in with investigative roles.

Process

- Develop a prioritization plan for the business areas that require continuous fraud detection. For example, should it be first applied to "low-hanging fruit" in common business process areas such as purchase-to-pay, procurement cards or T&E expense? Or to complex areas of greater fraud risk?
- Determine the appropriate frequency of tests for each detective activity. This often aligns with the timing of the relevant business process cycle. E.g., weekly or bi-weekly for payroll; daily, weekly or monthly for purchasing and payments.
- Assign responsibility of reviewing the results of the continuous fraud detection tests. Define the actions to be taken on continuous results.
- Create procedures for modifying tests when results indicate changes are required.
- Ensure source data validity and completeness. This is particularly important as the timely availability of the correct data is critical for continuous fraud detection.
- Determine procedures to be undertaken in the event that a test fails to run as planned.

Technology

- Keep in mind that technology issues most often relate to getting the appropriate data on an automated basis. When issues exist, start with confirming that the right data is available.

LEVEL 5 – MONITORING

With all of the building blocks of the preceding levels in place, an organization is well positioned to increase the benefits of audit analytics by expanding it to other business areas. Once your fraud team is regularly producing reports on control problems and proactively identifying potential instances of fraud through data analysis, then it usually makes sense to involve business process owners more directly and notify the appropriate individuals immediately of exceptions as they occur, so that they may respond appropriately.

By encouraging and supporting the implementation of continuous monitoring for fraud, the benefits of automated fraud detection techniques become obvious to a wider audience and start to be applied within the business. It is not unusual to hear a business process owner comment that they had been looking for

"Many companies start slowly, using off-the-shelf software to monitor select high-risk areas such as corporate credit-card purchases or accounts-receivable transactions. Others are integrating the monitoring into existing enterprise systems, for use by both operations and audit. The U.S. arm of Siemens Financial Services, which provides financing for health-care, energy, and industrial companies, has started running programs every night to monitor "everything that determines the value of a financial asset," namely, information on borrowers' riskiness, says Matthias Grossmann, CFO of the business unit. The decision to move to continuous monitoring was an easy one, he says, because the company was able to address the task with technology it already owned."

Quoted in "The 24/7 Audit"
CFO Magazine

some form of exception reporting system that provides greater insight into fraudulent activity or to improve overall oversight of their business area.

Continuous monitoring can also become an important component within an organization's risk management processes, helping to provide the business with a clearer picture of fraud risks, issues and trends.

Characteristics

The highest level of audit analytics occurs when the results of regularly repeated (continuous) testing of transactions and controls are provided directly to management for response. Continuous monitoring is a natural progression from continuous auditing, involving many similar processes and technologies. The main characteristic difference between Level 4 (continuous fraud detection) and Level 5 (continuous monitoring for fraud) are the workflow processes by which the business area is notified of exceptions and responds to them, as well as the use of dashboards for overall reporting of continuous monitoring results, status and trends.

At this level, the results of widespread testing can be accumulated and reported to show trends of risk areas and changing risks where, for example, a pattern of an increasing number of a certain type of exceptions becomes obvious.

Benefits

The greatest benefits from the use of analytics for fraud detection occur when the business process area has taken over responsibility for continuously monitoring for fraud and can address flagged issues as they happen. It is here where the ability to more effectively detect fraud starts to become preventative in nature. When people know that a given business area is being constantly and vigilantly scrutinized for fraudulent activity, the likelihood of people trying to commit fraud plummets. Fraud examiners can assess management response and remediation activities in order to determine what, or whether, additional fraud investigation procedures are required.

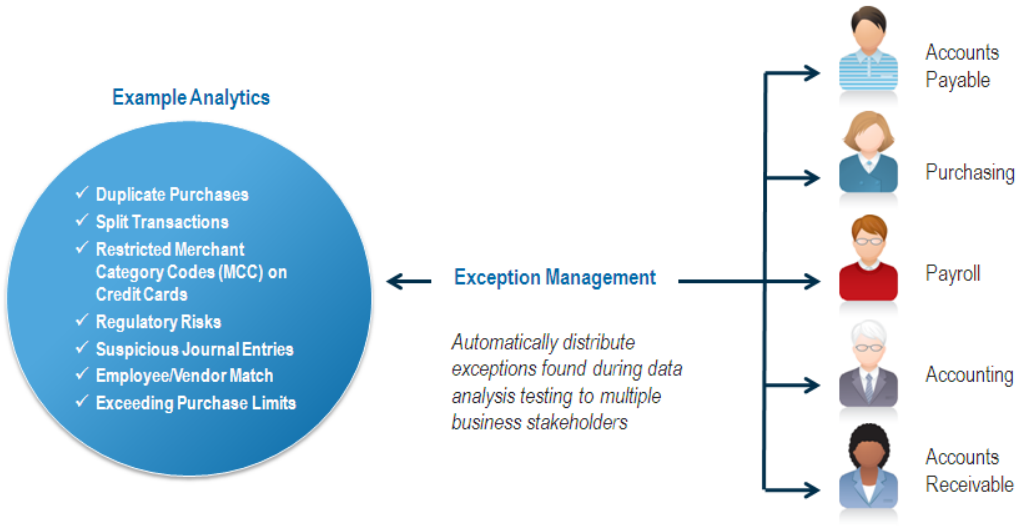
With continuous monitoring, organizations benefit from improved effectiveness of controls and require fewer control procedures since all transactions are monitored automatically. They experience a reduction in fraud – directly improving the bottom line and business performance, and reducing associated risks.

Continuous monitoring helps make the business more aware of the benefits of anti-fraud measures, thus creating a "fraud-aware business." It can also foster a closer working relationship between fraud examiners and business management regarding the impacts of risks and controls.

"AuditExchange will fundamentally transform how we manage spending and evaluate compliance. Reporting that was previously non-existent will now provide senior leadership with a clear picture of our control environment."

Hal Laughlin, IT Audit Manager
Dun & Bradstreet
(Recovered hundreds of thousands of dollars by identifying errors such as duplicate transactions and fraud.)

Figure 2: How Continuous Monitoring Works



Challenges

While an increasing number of organizations understand the benefits of continuous monitoring for fraud, there are various challenges in implementing and maintaining successful processes. This is usually because all of the required building blocks of processes, roles and technologies were not properly established or because management did not fully understand or accepts their critical role and responsibilities. False positives are also common. If continuous monitoring produces mass numbers of false or insignificant positives on an ongoing basis, the process will usually grind to a halt.

Organizational Risks

As with any system implementation process, there are risks that the project will not achieve the desired outcomes. For example, the continuous monitoring processes may not reveal any significant instances of fraud, even though from an assurance perspective it means that controls are working effectively. As a result, business owners may fail to see the value of the process and dismiss or terminate the program – a risk that could have a long-term negative impact.

How to Optimize

The following are areas that an organization should consider when looking to improve the effectiveness of analytics at the Continuous Monitoring level:

People

- Assign overall responsibility for the ongoing success of the continuous monitoring processes to an appropriate individual. This is a new business process, not simply a project.
- Allocate resources to the review and follow-up of exceptions according to the nature and severity of the exceptions identified.

Process

- Establish ownership of the roles in business management and for fraud examiners. Management must be able respond to the exceptions and resolve them where appropriate, usually by improving relevant processes and controls. Fraud examiners must be the ones to investigate suspected instances of fraud.

- The issue of false positives can be a significant one, especially if too many false positive exceptions are produced. Ideally, sufficient reiterative testing is performed to eventually eliminate false positives. Tests are modified to take account of specific transactions that fail a standard test but are not fraudulent in nature.
- Processes need to be established for response to continuous monitoring results – usually to the specific exceptions that are identified. This means fraud examiners investigating the indicators of fraud and management improving the defective control or behavior that allowed suspect activity to occur. Workflow and escalation procedures are usually needed in the event that an exception is not addressed within a certain timeframe.

Technology

- The technology requirements for continuous monitoring are very similar to those for continuous fraud detection, although usually with the addition of capabilities to support the management and reporting of exceptions and the workflow around their state of resolution.

CONCLUSION

This document provides an introduction to the Analytic Capability Model as it relates to fraud detection. Each organization will encounter unique challenges in optimizing the benefits at the different levels along with typical people, process and technology issues to address.

When continuous fraud detection is combined with continuous monitoring, it is possible to achieve an unprecedented level of fraud detection and prevention. However, it is also possible for organizations to function optimally at level 1 for the use of analytics in some fraud investigations or business process areas and at level 5 in others.

At a high level, the Analytic Capability Model provides organizations with a means of assessing their current level of use of analytics and identifying the desired level of use, together with a basic understanding of some of the issues to address. This model can be used as a roadmap to communicate plans, and to make the business case to management for building an analytic-enabled fraud detection strategy for the organization.

Overall, the model supports in making the business more aware of the benefits of fraud detection techniques, as well as helping them become more aware of what is happening within the business. By working through these levels, fraud examiners can increase the odds of a successful and immediately valuable adoption of analytical capabilities and to detect fraud sooner and with greater confidence.

COMPANY OVERVIEW

ACL Services Ltd. is the leading global provider of business assurance technology for audit and compliance professionals. Combining market-leading audit analytics software with centralized content management and exception reporting, ACL technology provides a complete end-to-end business assurance platform that is flexible and scalable to meet the needs of any organization.

Since 1987, ACL technology has helped organizations reduce risk, detect fraud, enhance profitability, and improve business performance. ACL delivers its solutions to 14,700 organizations in over 150 countries through a global network of ACL offices and channel partners. Our customers include 98 percent of Fortune 100 companies, 89 percent of the Fortune 500 and over two-thirds of the Global 500, as well as hundreds of national, state and local governments, and the Big Four public accounting firms. Visit us online at www.acl.com.

ACL Headquarters

T +1 604 669 4225
F +1 604 669 3557

■ acl.com
info@acl.com