PART 2: HOW TO COMBAT GOVERNMENT FRAUD, WASTE AND ABUSE
A FOCUS ON GOVERNMENT PROGRAMS
Protecting your reputation and the integrity of your mission
Protecting your reputation and the integrity of your mission
## CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud: it's big and it's complex</td>
<td>4</td>
</tr>
<tr>
<td>Is the problem just too big to address? Solving the government fraud issue</td>
<td>7</td>
</tr>
<tr>
<td>5 applications of technology to help combat fraud, waste and abuse</td>
<td>8</td>
</tr>
<tr>
<td>Process Flow</td>
<td>14</td>
</tr>
<tr>
<td>Fraud prevention across various government programs and payment areas</td>
<td>15</td>
</tr>
<tr>
<td>01: Improper Payments and Fraud in Entitlement and Welfare Programs</td>
<td>16</td>
</tr>
<tr>
<td>02: Healthcare Fraud</td>
<td>17</td>
</tr>
<tr>
<td>03: Education Fraud</td>
<td>18</td>
</tr>
<tr>
<td>04: Tax Evasion and Fraud</td>
<td>19</td>
</tr>
<tr>
<td>05: Procurement and Contractor Fraud</td>
<td>20</td>
</tr>
<tr>
<td>06: Cyber Security and Controls Over Data Protection</td>
<td>21</td>
</tr>
<tr>
<td>07: Fraud in Payroll and Employee Expenditure Systems</td>
<td>22</td>
</tr>
<tr>
<td>08: OMB A-123 and Internal Controls over Financial Reporting</td>
<td>23</td>
</tr>
<tr>
<td>Human data: Another very effective approach in the fight against fraud</td>
<td>24</td>
</tr>
<tr>
<td>Anti-fraud management technology buying guide:</td>
<td>25</td>
</tr>
<tr>
<td>What technology capabilities are needed to deliver the best results?</td>
<td>26</td>
</tr>
<tr>
<td>Conclusion</td>
<td></td>
</tr>
</tbody>
</table>
Getting a better handle on a serious problem

It’s no secret that fraud, waste and abuse in all levels of governments is a problem—and a big one. To some extent it is not surprising. Just think about the sheer number of different types of entitlement, healthcare and grant programs that exist at federal, state/provincial and local levels. Not to mention the complexity of the eligibility rules surrounding them. Trillions of dollars of payments are made to hundreds of millions of recipients. And similar size sums are collected from similar numbers of taxpayers.

Inevitably, mistakes will be made. Just as inevitably, some people are going to abuse the system and make fraudulent claims and evade taxes.

Then there are areas in which the public sector is similar to the private sector in terms of exposure to the risks of fraud, waste and abuse: vendors and contractors, along with other third parties, who abuse government purchasing and procurement systems. Often fraudsters work with the hope that, since government systems are so large and complex, their fraudulent activities are going to escape notice. Other forms of fraud and abuse also take place around systems for payroll, travel expenses and procurement cards.

And if all of this was not enough, those involved in audit, control and risk management within government are constantly facing new types of risks that have to be addressed. Consider cybersecurity and all the ramifications of data theft and privacy breaches, as just one example.

In terms of the damage caused overall by all of these issues, there is not only the problem of misuse and waste of government funds. Improper payments and all forms of fraud, waste and abuse, together with other control breakdowns, result in damage to the reputation of government agencies and give rise to unwanted media and political sensationalism.

In this eBook, we’ll look at how technology can make a real difference in the ongoing challenge of keeping fraud, waste and abuse under control across a variety of government areas. As data analysis has such a unique capability to address the problem, we will focus particularly on what it brings to the table. And we’ll try to demystify some of the complexities, so you can start getting a better handle on a serious problem, today.
Here are just some examples of the financial impact of the problem:

<table>
<thead>
<tr>
<th>Program</th>
<th>Agency</th>
<th>Total Payments (outlays)</th>
<th>Improper Payment Amounts</th>
<th>Improper Payment Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medicare Fee-for-Service</td>
<td>DHHS</td>
<td>$360.2B</td>
<td>$45.8B</td>
<td>12.7%</td>
</tr>
<tr>
<td>Earned Income Tax Credit (EITC)</td>
<td>DoT</td>
<td>$65.2B</td>
<td>$17.7B</td>
<td>27.1%</td>
</tr>
<tr>
<td>Medicaid</td>
<td>DHHS</td>
<td>$261.6B</td>
<td>$17.5B</td>
<td>6.7%</td>
</tr>
<tr>
<td>Medicare Advantage (Part C)</td>
<td>DHHS</td>
<td>$135.5B</td>
<td>$12.2B</td>
<td>9.0%</td>
</tr>
<tr>
<td>Unemployment Insurance (UI)</td>
<td>DoL</td>
<td>$48.4B</td>
<td>$5.6B</td>
<td>11.6%</td>
</tr>
<tr>
<td>Supplemental Security Income (SSI)</td>
<td>SSA</td>
<td>$55.4B</td>
<td>$5.1B</td>
<td>9.2%</td>
</tr>
<tr>
<td>Retirement, Survivors, and Disability Insurance</td>
<td>SSA</td>
<td>$824.2B</td>
<td>$3.0B</td>
<td>0.4%</td>
</tr>
<tr>
<td>Supplemental Nutrition Assistance Program (SNAP)</td>
<td>DoT</td>
<td>$76.1B</td>
<td>$2.4B</td>
<td>3.2%</td>
</tr>
<tr>
<td>Medicare Prescription Drug Benefit (Part D)</td>
<td>DHHS</td>
<td>$58.5B</td>
<td>$1.9B</td>
<td>3.3%</td>
</tr>
<tr>
<td>National School Lunch Program (NSLP)</td>
<td>DoA</td>
<td>$11.5B</td>
<td>$1.7B</td>
<td>15.2%</td>
</tr>
<tr>
<td>William D. Ford Federal Direct Loan Program</td>
<td>DoE</td>
<td>$102.1B</td>
<td>$1.5B</td>
<td>1.5%</td>
</tr>
<tr>
<td>Rental Housing Assistance Programs</td>
<td>HUD</td>
<td>$31.7B</td>
<td>$1.0B</td>
<td>3.2%</td>
</tr>
<tr>
<td>Federal Crop Insurance</td>
<td>DoA</td>
<td>$17.4B</td>
<td>$1.0B</td>
<td>5.6%</td>
</tr>
<tr>
<td>School Breakfast</td>
<td>DoA</td>
<td>$3.6B</td>
<td>$0.9B</td>
<td>25.6%</td>
</tr>
<tr>
<td>Pell Grants</td>
<td>DoE</td>
<td>$31.6B</td>
<td>$0.7B</td>
<td>2.2%</td>
</tr>
<tr>
<td>Children’s Health Insurance Program (CHIP)</td>
<td>DHHS</td>
<td>$9.5B</td>
<td>$0.6B</td>
<td>6.5%</td>
</tr>
</tbody>
</table>

U.S. GAO Testimony Before the Committee on Finance, US Senate, "Addressing Improper Payments and the Tax Gap Would Improve the Government's Fiscal Position"
At times the challenge of combatting government fraud, waste and abuse may seem overwhelming.

But as the old saying goes:

“How do you eat an elephant? ...One bite at a time.”
Even such a very large and complex problem can be broken down into more manageable pieces, and progress made one step at a time. And this is where technology has a particularly important role to play. Not only can software provide pointers to where to best focus efforts, but it can also provide a unique capability to find specific instances of fraud and abuse and then identify the root causes that can be fixed to reduce the problem in future.

In the private sector, for example, data analysis has proven to be of great value in reducing fraud and error. Look at credit card companies and how effective transaction monitoring has become in identifying suspect transactions. Look at how data analysis is being used to monitor and detect compliance issues around regulations for anti-money laundering, bribery and corrupt payments. Much of the initially overwhelming workload for public companies generated by the Sarbanes-Oxley Act has also been reduced dramatically by automated tests to determine the effectiveness of Internal Controls over Financial Reporting. Within federal government circles, the U.S. Department of Defense has been using data analysis for several years to analyze many billions of dollars of expenditures and reduce fraud and waste.

While data analysis is an important part of the solution to combatting fraud, software can also play a key role in managing the entire process of identifying and improving control weaknesses, as well as investigating and resolving specific instances of fraud and abuse.

The right technology can help put things into context, so that what may seem at times to be an insurmountable problem can be broken down and prioritized, and efforts concentrated on actions that have the greatest impact.
How to Combat Government Fraud, Waste and Abuse

Software tools can help you address fraud, waste and abuse in a number of ways. Here are the primary ones:

» Managing the process of identifying risks and control weaknesses
» Documenting the policies and controls that should be in place
» Data analysis and risk and control monitoring
» Dealing with red flags and ensuring the issues raised are addressed
» Gathering input and responses from across government agencies

Let’s start with looking deeper at each of these ways that technology can help by examining them in context of answering the questions that you need to ask in the fight against fraud.
Question 1.
How do we really understand the fraud problem and decide where to best focus our efforts?

The Answer: Risks and controls management and assessment

Before finding and tackling actual instances of fraud, waste, abuse and other control breakdowns, it is important to understand where the greatest risks lie and what policies and procedures are meant to be in place to prevent problems from occurring.

In the past, many government audit, inspection and control teams used tools such as spreadsheets, Word documents, emails, network file folders and BI tools to document control procedures, share information and identify where the greatest problem areas appear to lie.

It has become increasingly clear that this form of technology solution mash-up has a number of drawbacks. Not least among the challenges are actually managing an ever-growing mass of files, and ensuring that the correct versions are in use and that changes and updates are made without losing or corrupting data.

That is why many organizations have turned to specialized risk management and risk assessment software. These provide a better way for teams to map and document the “universe” of risks and corresponding controls in each area. Once identified, the risks can be assessed and ranked. This is an important starting point in making the decision as to where to focus efforts for audit, investigation, and remediation of problems.

Risk management software, which has much in common with audit management software, makes this process relatively simple. Different types of risk and control issues can be linked together where there are relationships. Software capabilities such as automated surveys and questionnaires can also be used to gather input from multiple contributors. The end result is the ability to look at up-to-date dashboards, reports and visualizations that provide insightful assessment of risk and control issues.
Question 2. How do we know which controls are working and which are breaking down (or just missing)?

The Answer: Data analysis

Being able to review a reliable assessment of the risk and control universe is a great starting point. The next issue is to get insight into what is actually happening: what is working well and what is in reality a problem? Auditors historically relied upon some form of sampling in order to test and then conclude on the effectiveness of controls. Data analysis fundamentally transformed this approach.

The basic concept is not complicated: Use data analysis technology to examine every transaction in an entire population of data (for example, everything that took place within a government program, payment system, or taxation system) to see if there are indications that fraud, abuse or other problems have taken place.

Test every transaction in multiple ways

An individual entitlement benefit claim, for example, can be examined in various ways to determine if the recipient is eligible. A basic test may be to compare claimant data with entries in the Social Security Administration’s (SSA) death file of deceased individuals. Another test could be to look for indicators that another, potentially duplicate claim, was made with similar data such as address or bank account information. A comprehensive series of tests can be applied to every claim or payment made in order to check its apparent validity.

Examine big data volumes to find unusual trends

Another form of analysis is to examine very large populations of transactions and look for trends and anomalies that indicate a potential problem area. Why, for example, are unusually high percentages of claims paid out by certain government employees, with very low denial rates? What trends can be seen that mean a problem is consistently worsening? Or what turns out to be far less of an actual problem than was originally thought?

Automated testing across multiple areas

Organizations that implement software to address the problems of fraud, waste and abuse often apply multiple analytics across a variety of process areas. Many end up with test libraries containing hundreds of tests that can be run as needed. In some cases this may mean daily or even hourly processing.

In other cases it is sufficient to perform testing on a less frequent basis: typically, weekly or monthly. Analytic tests can also be automated to run continuously, identifying exceptions and potential problems that require investigation on an ongoing basis.

The advantage of this approach—continuous monitoring, as it is often described—is that it provides timely notification of issues. Instead of a traditional audit approach in which testing is often performed long after transactions took place, risk and control specialists can get an immediate indication of a problem. Being able to respond more quickly increases the chances that the problem can be addressed—before it worsens.

“We don’t need to worry, we’ve got built-in controls in our claim and payment systems!”

- Famous last words

In an ideal world, every government claim and payment system would have built-in controls that reject any invalid claim before payment is made.

In practice, although it makes sense to include a range of key controls in an application system, it is very difficult to perform extensive analysis and testing in real time. The testing and investigation stages would soon make the entire claim payment process unacceptably slow and cumbersome.

However, when analysis is performed after the fact, it is relatively simple to determine where the primary control weaknesses are occurring. This provides a focus for determining what specific control improvements are required. It also means that types of claims that are fraudulent or invalid can be addressed and prevented from recurring.

Even if, for example, an ERP does have a series of built-in controls that limits the size of a payment to a vendor for goods and services, the control may be easily bypassed if the vendor simply submits multiple invoices just under the threshold limit. It is only by analyzing all payments to a specific vendor over time that this type of situation can come to light.
Question 3.
How do we best respond when we find a problem?

The Answer: Review and remediation of flagged results

One of the biggest practical challenges of using data analysis and monitoring is that it uncovers many things and provides many insights. Someone needs to examine the results—specific “exceptions” and anomalies, trend reports, or whatever is the intended output of transaction monitoring systems—and decide what needs to be done. This is where things have the potential to turn into something of a quagmire of potentially very important information...that no one is actually using.

Software for managing issues and their resolution—whether at a very detailed transaction level, or at a higher control and policy level—is critical. The results of testing are shown visually and can be examined in many ways in order to better understand where the real problems lie and what causes them.

Automated workflow means that specific types of exceptions and results are routed electronically to appropriate individuals for resolution. If responses do not take place, or are inadequate, the issues can be escalated to a more senior level.
Question 4.
How do we track where we are right now in this overall process?

The Answer: Ongoing risk assessment and status reporting

Software not only manages the workflow, but also allows the entire process to be reviewed and the current status of all monitoring activities to be illustrated and quantified. This is where software also plays another uniquely powerful role: it provides the ability to see a current assessment of the entire universe of risks and control effectiveness.

This means, for example, a visual color-coded heat map of risks, as well as drilldown capabilities to see the detail of specific issues. It also means the ability to report, for example, that $X billion of claims payments were examined and Y%, representing $Z million, were found to involve specific forms of fraud and abuse. Of these, A%, or $B, resulted in recovery of funds and improvements in control procedures.
Question 5.
How do we efficiently gather important input from individuals throughout government agencies?

The Answer:
Surveys, questionnaires and analysis of people responses

In addition to the insights gained from analysis of payments, it is also important to have a current understanding of what is happening based on the input of those working in the front lines.

Software that supports automated surveys and questionnaires can gather large amounts of information directly from individuals in different roles across the government spectrum and rapidly interpret what is found. Analysis of people responses to fraud and abuse issues is a new and rapidly developing area in the world of risk and control management.
Dealing with fraud, waste and abuse in government payment programs involves a number of important stages, which preferably should be linked together into an integrated process. Here are the logical steps in an overall approach to addressing the problem. It is a model that can be used for managing a range of risk and control issues—not just around fraud, waste and abuse. Software plays a key role in each stage of the process.

**PROCESS FLOW**

Dealing with specific instances of fraud, waste and abuse and deciding how to strengthen controls

Of findings and results

Data analysis plays a key role in testing controls and finding problem payments

Intended to reduce the chance of fraud, waste and abuse from occurring

Determine which are the most significant problems - often supported by ranking and survey questionnaires

Description and log record of specific analytic and other procedures performed

Improve the process overall

Categorize the different types of risks that can lead to fraud, waste and abuse in payment programs

**IDENTIFICATION**

**IDENTIFICATION**

**ASSESSMENT of Risks**

**ASSESSMENT of controls effectiveness**

**MANAGEMENT**

**DOCUMENTATION**

**REPORTING**
In this section we’ll look at just a few of the ways in which software, particularly data analytics, can be used to reduce fraud, waste and abuse in a range of government programs and payment areas. Although the exact nature of applications will vary from one program to another, many of the techniques and types of tests (for example, matching claims and payment data with data from other sources) are similar across most programs.

In addition to data analysis and transaction monitoring, there is also a lot of similarity across areas in the way that software can be used to:

- manage risks and controls
- document procedures
- resolve and remediate weaknesses
- perform ongoing assessments

FRAUD PREVENTION ACROSS VARIOUS GOVERNMENT PROGRAMS AND PAYMENT AREAS
01: Improper Payments and Fraud in Entitlement and Welfare Programs

Let’s take a closer look at some government programs and critical payment areas where analytic technology can be applied in the fight against fraud, waste, and abuse.

E.g. Unemployment Insurance

The Federal-State Unemployment Program is estimated to have an improper payment rate of close to 12%, which currently means over $6.5B of taxpayer dollars. According to the National Association of State Workforce Agencies’ Unemployment Insurance Integrity Assessment Report, only 32% of states use fraud detection software—even though it is one of the most effective ways of uncovering improper payments.

Here are some ways in which data analysis software can detect fraud and abuse in UI payments. Many of them are based on comparing data between two systems to find indicators that a recipient is ineligible for UI:

- check for duplicate claims by identifying multiple addresses for the same SSN in a given timeframe
- compare claims to other databases to identify unreported earnings or existing employment. For example check claimant details to the National Directory of New Hires (NDNH) or State Directory of New Hires (SDNH)
- match UI claimant data with data from registries of deceased individuals in State Vital Records Department databases
- analyze prison records to cross-match UI claimants
- match claims to Department of Motor Vehicle records to confirm positive verification, as well as find claimants who also happen to own multiple luxury vehicles
- identify claims using foreign IP addresses or to “hot” IP addresses known for fraudulent claims
Healthcare Fraud

Fraud in government funded healthcare is known to be of huge proportions. Although both healthcare providers and beneficiaries are known to be involved in Medicare and Medicaid frauds, a relatively small number of medical practitioners and other service providers are known to be responsible for the highest percentage of cases.

Data analysis is increasingly acknowledged as one of the most effective ways to shed light on offenders. The following are typical types of analytic tests designed to detect instances of fraud:

Medicare and Medicaid
- search for duplicate billing by matching procedures billed by care facilities and also billed directly by medical practitioners
- compare distribution of billing codes compared to averages to identify instances of “upcoding” by healthcare providers
- analyze instances of multiple procedures claimed for a given patient within a specific time period to find “unbundling” activities

Affordable Care Act
- match applicant data with other database information to detect fake applicants
- match applicant income declarations to other income and taxation data sources to detect understated income levels
03: **Education Fraud**

Fraud in education systems is carried out both by students and academic institutions. One of the most common forms of fraud occurs when a school or student submits false information in order to receive federal student aid.

Some examples include:

- manipulating student loan default rates by completing fictitious loan deferment applications
- falsifying academic records of students in order to obtain loans or grants
- using false or using stolen identities to create fictitious student enrolments in order to qualify for loans or grants
- providing false information on income in order to apply for grants

There are several types of transactional and data analysis tests that are effective in identifying false submissions that do not reconcile with data from other independent sources, including example tests such as:

- comparing income declarations on grant applications to IRS records
- checking student personal data, such as name, address and SSN details to taxation, DMV and other databases
**Tax Evasion and Fraud**

Data analysis is used globally by taxation authorities, at both national and regional levels, in their role of ensuring that taxpayers comply with rules and regulations.

As is the case in many areas of fraud, some of the most effective techniques for uncovering fraudulent tax returns include comparing declared income and expense submitted information with independent data sources for payments and revenues. For example, income declared by an owner-managed business or contractor can be matched to expenses claimed by another taxpayer. Data analysis is also very effective in performing statistical analyses to determine statistical norms for income and deductible expense levels and to identify outliers for investigation. Similar methods can also be applied in the case of sales tax fraud and evasion.

One common form of tax fraud in the retail business involves software that suppresses evidence of some sales from Point of Sale systems in order to understate revenues (“POS Zapping”). This form of fraud can be detected by using software to match POS records of sales to bank records of cash deposits, as well as to changes in inventory levels.

**Other examples tests include:**

- comparing claims for interest expense deductions with income revenue data from financial institutions
- matching investment income declarations with bank records
- comparing deduction claims for unreimbursed medical expenses with data from of health care insurance providers to determine if reimbursements were actually made
05: Procurement and Contractor Fraud

While a lot of attention is paid to fraud and abuse in government welfare, healthcare and other entitlement programs, governments also typically spend massive amounts on construction and infrastructure products. As in any large business in the private sector, this opens up many possibilities for frauds that are carried out by third parties such as vendors or contractors.

Here are some tests typically applied to uncover various fraud schemes:

- compare payments to contract terms and records of delivery of goods and services
- test to determine if procurement and payment approval controls are circumvented by “splitting” transactions into smaller amounts just under a manager’s approval limits
- find payments to fictitious contractors and vendors by checking validity of SSNs and tax IDs
- look for matches between vendor payment data and employee data to find “phantom vendor” schemes
- identify attempts to bypass controls by short term unauthorized changes to vendor bank account data, or to manager’s payment approval limits
- look for fraudulent invoices by checking details to records of goods and services provided
- analyze payment data to determine instances of unusually high charges for goods and services when compared to averages
Cyber Security and Controls Over Data Protection

Risks from cyber security breaches are often ranked among the highest that organizations face. The damage that can be caused by data theft or breakdowns in data privacy is considerable. In the government sector the impact is not necessarily a great financial one, as is often the case in the private sector, but can have huge ramifications in terms of negative media exposure and loss of reputation, as well as potential legal liability.

Analysis and monitoring technology is particularly effective at testing for indicators of access control weaknesses, as well as actual incidents of unauthorized access to networks, applications, and databases. Such analyses may highlight attempts to bypass controls by employees and contractors. They may also identify attempts by outsiders to hack into systems.

Some specific examples of analytic tests includes:

- look for instances in which an application control setting is changed and then reversed back to its original state within a short time period (e.g., approval authorization settings, customer credit limits, duplicate payment checks)
- test application access by terminated or vacationing employees
- analyze application settings to identify unusual high risk combinations and inappropriate access levels
- identify direct database changes, bypassing application controls
- test access to applications, networks and other systems at unusual times
- compare and combine analyses of actual access to applications, networks and databases to highlight unauthorized and high risk activities
- analyze weaknesses in SOD settings compared to actual SOD violations
- identify any “super-user” administrative access and bypass of standard password controls
- compare access violation analyses performed by audit teams with analyses performed by IT staff with proprietary security software
Fraud in Payroll and Employee Expenditure Systems

Payroll is obviously another very large expense area for governments. Although fraud and abuse are unlikely to be on the same scale as some other forms of fraud and abuse, payroll risks need to be considered, along with other areas involving internal controls over employee-related expenses, such as travel and entertainment (T&E) and the use of procurement cards (P-cards) by government staff.

Here are some typical analytics used to look at each finance area:

**Payroll**
- analyze data to identify abnormally high overtime payments
- match data to determine payroll amounts paid to individuals who have left government employment or are deceased
- identify “phantom” employees by matching data to indicators of actual employee activity

**Procurement Cards (P-Cards)**
- identify expenditures on items typically associated with personal use by looking for merchant codes, vendor names and key words that are associated with non-business items and services
- identify transactions made on weekends, holidays or while the employee is on vacation
- identify split transactions in which a large purchase is paid for in smaller amounts, just under a review/approval threshold
- test for purchases of the same item or service within a specific timeframe (i.e., One purchase may be legitimate, the other may be intended for personal use)
- check for duplicates in cases where a P-Card was used for a specific purchase and the same purchase was processed as a T&E claim

**Travel and Entertainment**
- compare claims data to uncover claims by multiple employees for the same expense
- compare dates of expense claims with HR records for employee vacation dates
- analyze claims to find expenses relating to airfares and hotels in non-standard locations (e.g., vacation resorts)
- identify claims for meals for multiple persons made on the same day and at the same location as claims made by other employees
- find duplicate claims by matching charges made through procurement credit cards as well as through a travel reimbursement claim
- search for expense claims including vendor names and key words that are associated with personal use items and services
- identify airfare payments/claims for which there are no corresponding hotel or meal charges
- check for instances where mileage claims were made for the same time period as car rental charges or other transport costs
08: OMB A-123 and Internal Controls over Financial Reporting

Requirements for testing Internal Controls over Financial Reporting (ICFR) can be as resource intensive for audit and control specialists in government as for their counterparts in the private sector. The good news is that technology is now well proven as a method of reducing the burden of regular testing. Compliance with OMB circular A-123 can be achieved in large part by automating key control tests through the use of transaction analysis.

To learn more, download ACL's free eBook.

The essential guide to seriously reducing the burden of ICFR/SOX/A-123 compliance
HUMAN DATA: ANOTHER VERY EFFECTIVE APPROACH IN THE FIGHT AGAINST FRAUD

Analyzing very large volumes of data is a well-proven method of finding fraud, waste and abuse in government programs and payments. Another effective approach—one that has been around for a lot longer than computer technology—is whistle blowing by individuals who report problems of which they have become aware.

Whistleblower programs
Hotlines and other forms of whistleblower reporting systems are among the most effective means for detecting certain types of fraud and abuse. Software provides the ability to gather information anonymously and then connect the reported incidents into other components of risk and control systems. Individual reports from hotlines and whistleblower reporting websites, for example, can be linked to an assessment of a particular type of risk exposure or control effectiveness. They can also be aggregated into a central repository and included in overall risk status reporting dashboards.

Reported incidents can also be connected into a full escalation management process, where certain conditions can instantly be flagged and broadcast to investigators for review. Aggregated data with associated comments and resolution efforts can be analyzed with visualization tools to gain insight into trends and areas of greatest risk.

Pre-approval of gratuities and potential conflicts of interest
Software’s ability to automate the process of collecting and connecting data gathered from questionnaires and surveys is also effective in other application areas. For example, government employees can be encouraged to report benefits offered by vendors and get approval in advance to prevent conflict of interest, bribery and corruption. Again, this information can be linked to the relevant controls in a risk and control database, providing 360° oversight by combining pre-approval controls with detective controls.

Figure 1: Creating a questionnaire to collect information from employees
ANTI-FRAUD MANAGEMENT TECHNOLOGY BUYING GUIDE:
WHAT TECHNOLOGY CAPABILITIES ARE NEEDED TO DELIVER THE BEST RESULTS?

✓ Modern Interface and Platform
Earlier generations of audit and risk management technology, many of which are still available, tend to be based on applications that require considerable configuration and are complex to implement and use. Current technologies for audit, fraud detection and risk management have advanced as rapidly as software in the general consumer market—transforming the implementation challenge into a simple and rapid process. Usability has also taken huge strides with interfaces that are as genuinely intuitive.

Portability is another feature of modern audit and risk software, supporting use not just on desktops and laptops, but on tablets and phones. This enables auditors and control specialists the ability to gather and access information, as well as perform testing and processing without being tied to an office or desk.

✓ Integrated Support of all Aspects of Audit, Risk and Control Processes
It is still the case that older technologies tend to have compartmentalized functionality with separate software product components for different aspects of audit and risk management processes. While these usually support data exchange between components they are often not closely and consistently integrated. For example, in legacy systems, analytic capabilities are provided by separate products that are not closely integrated with specific risk and control functionality.

On the other hand, modern software products offer a high degree of integration, with seamless integration of functionality for:
- Defining and documenting risks and controls
- Assessing and ranking risks
- Assessing and testing control effectiveness
- Analyzing transactions and data
- Investigating results
- Managing exceptions
- Remediation and escalation workflow
- Data and test repositories
- Dashboards and reporting

✓ Data Analysis and Monitoring
Data analysis software designed specifically for detection of fraud, waste and abuse has specific functional capabilities. In general, these capabilities are similar to those for data analysis in audit or for other risk and control testing purposes.

Look for:
- Pre-built analytic routines, such as classification, stratification, duplicate testing, aging, join, match, compare, as well as various forms of statistical analysis, including Benford analysis, all of which have a role to play in helping to find fraud indicators
- Data manipulation function capabilities for combining, matching, extracting data
- Data visualization—to spot unexpected anomalies and to provide new insights
- Ability to access a broad range of data sources and types
- Support of full automation and scheduling of analytics
- Ability to perform complex testing and fraud detection
- Comprehensive logging of all procedures performed (which is important in generating complete audit trails to support detailed investigation)
A technology-driven approach to managing government fraud, waste and abuse

It is well known that technology can now play a critical and transformative role in addressing many of the largest problems facing the world. This is equally true in the world of government audit and risk management, including fraud, waste and abuse.

The role of the government auditor and others responsible for integrity in government programs and systems is not an easy one. But technology can now help these professionals to make a real difference. The challenges do not have to be insurmountable just because they are extremely big. Embracing the right technology strategy can transform the impact of even the smallest audit and risk management teams. Starting in a relatively small way can soon lead to increasingly big steps in dealing with a large problem.

Has the time come to take a closer look at how good a job your department is doing in using technology to deliver on its mandate?

Let us help.

ACL’s comprehensive platform with integrated analytics helps mitigate risks, identify opportunities for cost savings, and stop fund leakage. We’ve drawn upon two decades of experience working with 200+ departments in 37 national governments worldwide, and 500+ regional, state and local governments to develop detailed methodologies and best practices.

For a free assessment of how you can get the oversight you need on government programs and payment areas, call 1-888-669-4225 or email info@acl.com
Visit the Public Sector section in ACL Inspirations for hundreds of analytic ideas built from decades of experience from ACL initiatives worldwide.

Get inspired at www.acl.com/scripts
About the Author:
John Verver, Advisor to ACL

John Verver, CPA, CISA, CMC is an acknowledged thought leader, writer and speaker on the application of technology, particularly, data analysis, in audit, fraud detection, risk management and compliance. He is recognized internationally as a leading innovator in continuous controls monitoring and continuous auditing and as a contributor to professional publications. He is currently a strategic advisor to ACL, where he has also held vice president responsibilities for product strategy, as well as ACL’s professional services organization. Previously, John was a principal with Deloitte in Canada.

About ACL

ACL delivers technology solutions that are transforming audit, compliance, 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