Galvanize

Combating government fraud, waste, & abuse

A getting started guide

Table of contents

GOVERNMENT FRAUD, WASTE, & ABUSE

A really big problem

It's an unfortunate reality that every government organization is vulnerable to fraud committed by employees. Fraud is especially common in purchasing cards (P-Cards) and travel and entertainment (T&E) expenses. Both involve massive volumes of transactions, making it easier for fraudsters to avoid being discovered.

On top of this employee fraud, unintentional waste and abuse also happens. For example, the US Government Accountability Office[1] estimates that improper payments in government programs totaled $141 billion in 2017.

A lot of this fraud and waste occurs within government programs like unemployment insurance, healthcare, and social security.

Even with strict policies, procedures, and controls in place, it's impossible to stop all instances of fraud. But it is possible to find indicators—those data trails inside millions of processed transactions—that can help you act faster.

It's proven that purpose-built data analytics technology reduces instances of fraud, waste, and abuse. According to the Association of Certified Fraud Examiners[2], government organizations using data monitoring and analysis software saw 52% lower losses, and experienced 58% faster detection of fraud occurrences.

In this eBook, we'll show you how to use data analysis as a continuous system for detecting fraud, waste, and abuse, and provide ways to specifically examine T&E fraud, P-Card abuse, and program waste.

[1] *US Government Accountability Office, 2017, https://www.gao.gov/key_issues/reducing_government-wide_improper_payments/issue_summary*

[2] *Association of Certified Fraud Examiners, 2018, 2018 Global Study on Occupational Fraud and Abuse*

How is data analysis used to detect government fraud?

There are two primary ways to use data analysis to detect fraud, waste, and abuse.

01

Analyze entire populations of transactional data to look for anomalies. This doesn't necessarily prove that fraud or abuse has occurred, but it's an effective way to flag situations that just don't make sense and need further investigation.

For example, why should one government contractor, providing essentially the same goods and services as a hundred others, be paid 50% more than the average? There could be several valid reasons, but if none are obvious, it's possible that fraud has occurred.

02

Analyze transactions for indicators of known risks of fraud, waste, and abuse. For example, an employee may be authorized to use a P-Card for purchases of specific business items. If an analysis of P-Card data shows that a series of purchases were made from a home renovation store or high-end clothing store, this could be a strong indicator of actual fraud.

A really effective way to uncover fraud is to compare data across different databases and systems. One example is to compare procurement and payments information with human resources records (e.g., bank account and other personal data) to see if there are indications of an employee “phantom vendor” scheme.

You could also test to see if enterprise resource planning (ERP) application control settings have been changed. For example, test to see if any manager with a $5,000 approval limit for purchase orders had that authorization limit changed briefly to allow fraudulent activities, and then reverted back to $5,000.

What you need in a data analysis tool

Unlike trying to crunch numbers in an Excel document or across multiple, siloed platforms, purpose-built fraud detection and data analysis software has specific capabilities. It's similar to software that's used in audit or for other risk and control testing purposes.

HERE ARE FIVE THINGS YOU'LL WANT WHEN CHOOSING YOUR SOLUTION.

01 Pre-built analytic routines like:

+ Classification
+ Stratification
+ Duplicate testing
+ Aging
+ Joining
+ Matching.

02 Data visualization, to uncover unexpected anomalies more easily and provide additional insights.

03 Automated detection and prevention, and the development of complex tests to detect and address the more sophisticated types of fraud.

04 Procedure logging, which generates complete audit trails that may be required to support detailed investigations.

05 Data access and manipulation, which accesses, compares, cleanses, and combines data from almost any source—without modifying the source.

5 ways to combat fraud, waste, & abuse

Software tools are designed to address fraud, waste, and abuse by helping you:

+ Manage how risks and control weaknesses are identified.
+ Document the policies and controls that should be in place.
+ Conduct data analysis and risk and control monitoring.
+ Deal with red flags and make sure the issues raised are addressed.
+ Gather input and responses from multiple government agencies.

01 Risk & control management & assessment

Before finding and addressing actual instances of fraud, waste, and abuse, you have to pinpoint where the greatest risks lie.

It's also important to outline the required policies and procedures to prevent these problems from occurring.

In the past, many government audit, inspection, and control teams used things like spreadsheets, Word documents, emails, and network folders to document control procedures, share information, and identify the greatest problem areas.

But these solutions have drawbacks, including the challenges of managing an ever-growing mass of files, version control issues, and data corruption/loss.

Spreadsheets and legacy software are not good at giving a comprehensive view of the interconnected relationships across your risks and controls. Software that's purpose-built better integrates risk and control definitions, assessments, and testing, so you can quickly understand the big-picture status of all of your risks and controls.

When you get out of spreadsheets and adopt technology, you can start to:

+ Map risks to corresponding controls in each area.
+ Rank risks according to priority and choose areas of focus.
+ Gather input from multiple contributors through surveys and questionnaires.
+ Uncover deep insights into risk and control issues through up-to-date reports and visualizations.

02 Advanced data analytics

How do you know if your controls are working well? Traditionally, you would sample-test your controls, but that's risky, as only some transactions get tested, and others don't. This is where advanced data analytics become critical.

TEST EVERY TRANSACTION MULTIPLE WAYS

A comprehensive series of tests can be applied to every claim or payment to check that they're all valid. For example, an entitlement benefit claim can be examined in various ways to determine if the recipient is eligible.

+ Compare claimant data with entries in the Social Security Administration's Death Index to identify deceased individuals.
+ Look for indicators that a duplicate claim was made using similar data (e.g., address or bank account information).

AUTOMATE TESTING ACROSS MULTIPLE AREAS

Advanced data analytics can apply multiple tests across a variety of process areas. Analytic tests can also be automated to run continuously, identifying exceptions and potential problems that require investigation on an ongoing basis.

Unlike the traditional approach where testing happens long after transactions have occurred, your risk and control specialists get notified of problems much sooner, so they can be addressed before they get worse.

EXAMINE BIG DATA VOLUMES TO FIND UNUSUAL TRENDS

Data analytics let you examine very large populations of transactions and look for trends and anomalies that could indicate problems.

For example:

+ Why 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 worsening?
+ What is actually less of a problem than originally thought?

03

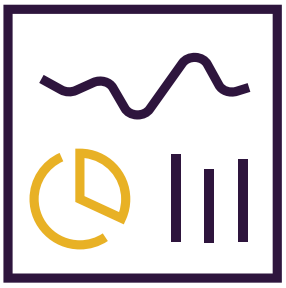
Review & remediation of flagged results

Sure, data analytics and monitoring provide useful insights, but now you've got the challenge of actioning them.

Someone needs to examine the results—specific exceptions and anomalies, and trend reports—to decide what needs to be done. This is where things can get intensive and messy. But there are software tools specifically designed to manage these issues (and their resolutions) with built-in best practices and workflows.

Workflows direct specific exceptions and results into the hands of the right people for follow-up. If there's no response within a set time frame, the issues get escalated to someone in a more senior role, to make sure nothing gets missed.

Another excellent feature of fraud detection software is dashboards, which summarize the results of analysis and test processing over time. Senior management uses these dashboards to review trends of exceptions identified, and the status of unresolved or under-investigation items.



04

Ongoing risk assessment & status reporting

When you use analytics to measure risk, you'll probably find the more data you collect, the harder it is to make sense of it all. Here's where something like risk scorecards or risk heatmaps help.

These tools, found in risk management software, make sense of all that data by visually displaying a current assessment of all your risks and control effectiveness in real time.

Risk heatmaps make it possible to plot your organization's fraud threats and help visualize the various types of financial, regulatory, and reputational impacts that these frauds could have.

On the right are two examples of how HighBond's risk heatmaps display risks visually, along with rankings and related issues.

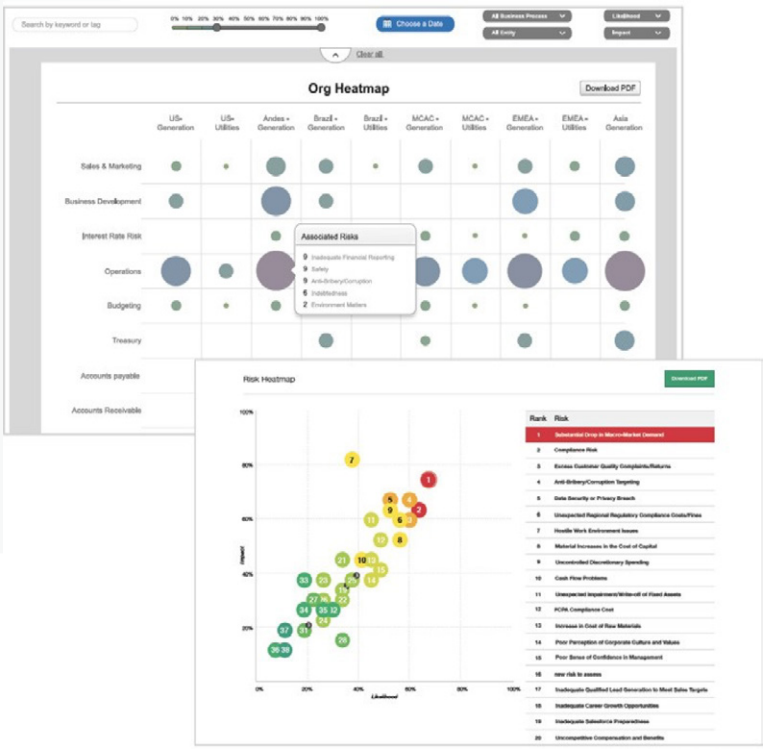


FIGURE 1: EXAMPLE HEATMAPS IN THE HIGHBOND PLATFORM.

05 Surveys, questionnaires, & whistle-blower hotlines

Your front-line employees are the ones who deal with risk each day, and they're often in the best position to provide feedback to senior management about fraud-related risks.

Software with built-in surveys, questionnaires, and whistle-blower hotlines gives you an understanding of what's happening in your organization based on feedback from these front-line workers.

This feedback becomes data, and the data gathered from questionnaires and surveys can help uncover issues or solutions in other areas of the organization. For example, employees who would like to receive a gift or benefit from a vendor can report the benefit and get approval in advance to prevent conflicts of interest, bribery, and corruption.

Plus, employee tips are the most common initial detection method. Organizations with hotlines detect more fraud more often—46% compared with 30% in organizations that don't have hotlines.[3]

Building an anonymous web hotline inside your software platform allows employees, contractors, and vendors to safely report suspicious behavior, helping you more quickly identify potential fraud.

[3] *Association of Certified Fraud Examiners, 2018, 2018 Global Study on Occupational Fraud and Abuse*


4921
4921
VALID FROM
02/0
MRS
1 2 3

Identifying purchasing card & T&E fraud

More and more, P-Cards are being used to reduce the costs of traditional procurement processes.

While this makes a lot of sense in terms of efficiency and effectiveness, P-Cards are particularly prone to fraud and abuse because they're so easy to use.

In government organizations where employees use credit cards for T&E, the types of fraud—and the ways to identify them—can be very similar to those for P-Cards.

In some cases, employees might get credit cards for both purchasing goods and services and for T&E expenses. In other cases, employees submit expense reports for reimbursement. Both methods are full of opportunities for fraud and abuse.

Let's look at some common P-Card and T&E tests for identifying fraud.

01 Purchasing card fraud tests

Here are examples of some common data analysis tests used to identify indicators of P-Card fraud.

PURCHASES OF ITEMS INTENDED FOR PERSONAL USE

Analytics tests:

+ Analyze transactions to look 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.

DUPLICATE PURCHASES

Analytics tests:

+ Identify multiple purchases of the same item or service within a specific time frame. (One purchase may be legitimate, the other may be intended for personal use.)
+ Identify where a P-Card was used for a specific purchase and the same purchase was processed as a T&E claim.

UNUSUAL USAGE PATTERNS

Analytics tests:

+ Look for P-Card holders whose usage is abnormally high—both in cost and frequency—compared to others in a similar role.
+ Identify P-Card holders with unusually large cost limits on their cards.

FUEL CARDS

Analytics tests:

+ Look for fuel card usage that is abnormally high compared to others in a similar role.
+ Calculate expected mileage for a particular volume of fuel charged and compare to typical or expected travel patterns.

02
Travel & entertainment fraud tests

Here are examples of some common data analysis tests you can use to find fraudulent T&E expense claims.

CLAIMS FOR PERSONAL EXPENSES

Employees, especially those who travel frequently, may be tempted to charge airfares, hotels, and meals for personal use—knowing it can be hard for an approver to determine if a trip was for business purposes.

Analytics tests:

+ Identify expenses relating to airfares and hotels in non-standard locations (e.g., resorts).
+ Identify expense claims with vendor names and key words associated with non-business items and services.
+ Identify expense claims during employee vacations.

DUPLICATE CLAIMS

Analytics tests:

+ Identify claims for meals for multiple people made on the same day and at the same location as claims made by other employees.
+ Identify expenses incurred using both a company credit card (P-Card or general corporate card), as well as through a reimbursement claim.

UNUSUAL USAGE PATTERNS

Analytics tests:

+ Look for patterns of unusually large or frequent T&E claims compared to employees in a similar role.

REFUNDED OR INFLATED EXPENSES

A fairly common T&E fraud involves employees paying for or claiming flights, conferences, or training courses through a T&E system and then canceling the transaction. Instead of reversing the T&E charge, the employee receives the refund amount.

Another fraud involves purchasing a business class airfare and then changing to an economy ticket, receiving the refund personally.

Analytics tests:

+ Identify airfare payments/claims for which there are no corresponding hotel or meal charges.
+ Identify claims for off-site conferences or courses with no corresponding T&E charges.

CAR MILEAGE CLAIMS AND FUEL EXPENSES

Fraudulent schemes related to car travel expenses can range from over-stating mileage to duplicate claims of both mileage and public transport or car rentals.

Analytics tests:

+ Identify instances where mileage claims were made for the same time period as car rental charges or other transport costs.
+ Identify total car mileage claims and compare to distances of reported business travel destinations.
+ Identify instances where claims for mileage and fuel are both made in the same time frame.

Identifying programs fraud

Government departments provide a range of entitlements, benefits, and subsidies to organizations and individuals.

These payments total billions of dollars per year. The problem is that the nature of many government programs makes them particularly susceptible to fraud, waste, and abuse.

Data analytics and continuous monitoring, as well as software for risk and control management, can help reduce and contain the numbers of improper payments that inevitably occur.

Let's take a look at some analytics tests in common program areas.

Programs fraud tests

These are just a few examples of the many types of analysis tests you can apply to specific government programs to detect fraud, waste, and abuse.

01 Health insurance/benefits

Phantom billing

Suppliers may be billing for goods not actually ordered or received.

Analytics test:

+ Identify suppliers having an unusual number of billing codes, compared to suppliers of a similar size/type.

02 Unemployment

Identity theft and impostors

Personal information is stolen and used inappropriately to apply for benefits.

Analytics tests:

+ Identify benefits paid to multiple addresses for the same national insurance number.
+ Identify benefits paid to multiple addresses within a short time period.

03 Income tax

Inflated, inappropriate, or fictitious deductions

Distributions of the first digits of numbers on a tax return should follow Benford's law,[4] but often the number of values isn't large enough for statistical relevance. An unusual distribution pattern of numbers within the values on filed returns can be an indication of inflated, inappropriate, or fictitious deductions.

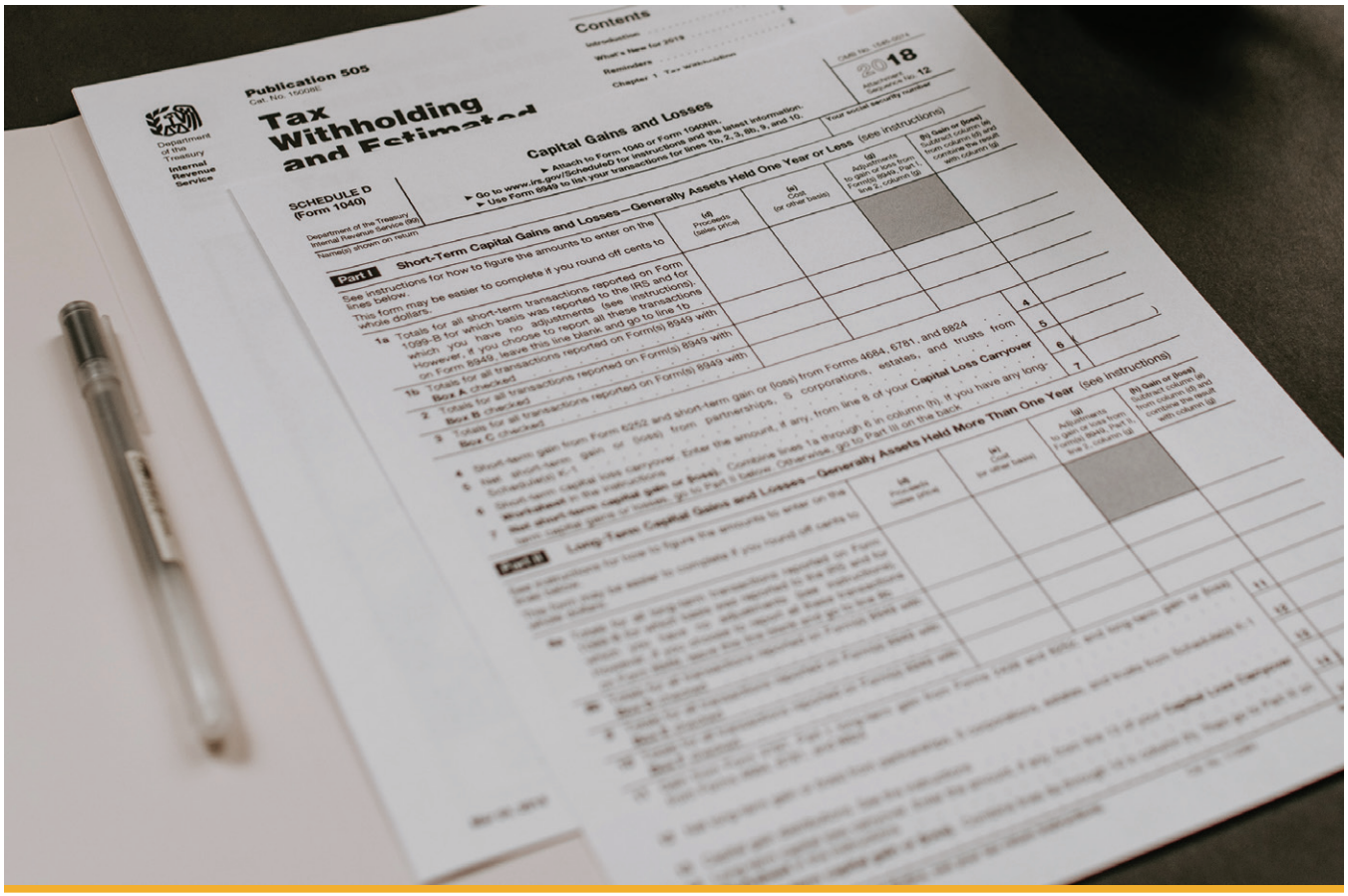
Analytics test:

+ Numeric digit analysis: Calculate the distribution of frequencies of digits used in the tax return, and identify unusual distributions of numeric digits.

04 Sole proprietorships misused to conceal and misdirect income/deductions

Analytics test:

+ Sole proprietor industry metric analysis: Calculate key metrics for sole proprietors based on industry codes, such as income/expense/equity ratios and cash ratios. Flag sole proprietors that have unusual metrics compared to similar sole proprietors of the same industry code.



[4] https://en.wikipedia.org/wiki/Benford%27s_law

Steps to create a fraud monitoring process

01

Define the overall objectives. Specifically define whether the fraud detection process is part of an overall risk management and control testing strategy, part of a regular internal audit process, or a standalone function.

02

Identify and define the specific fraud risks to be tested—effectively creating a "fraud risk universe."

03

For each risk, identify and define a data analysis fraud detection test in terms of:

+ Data requirements
+ Data access processes
+ Analysis logic.

04

Coordinate with the IT department (or external vendors in the case of P-Card or credit card data) as needed for issues of data access and any centralized processing requirements.

05

Build the analytics tests.

06

Validate the effectiveness of those tests.

07

Establish timing and responsibilities for automated test processing.

08

Establish workflow and responsibilities for exception management and resolution.

09

Implement reporting processes.

10

Having started with a core set of relatively straightforward tests, progressively build and implement a broader "library" of more specific tests that address your unique fraud risks.

Let us help you enhance your fraud detection and prevention program.

To find out how Galvanize can help your organization mitigate fraud, waste, and abuse, identify risks and opportunities for cost savings, better protect taxpayer funds, and prevent funds leakage, call 1-888-669-4225, email info@wegalvanize.com, or visit **wegalvanize.com**.

Galvanize

About the Author

John Verver

CPA CA, CMC, CISA

John Verver is a former vice president of Galvanize. His overall responsibility was for product and services strategy, as well as leadership and growth of professional services.

An expert and thought leader on the use of enterprise governance technology, particularly data analytics and data automation, John speaks regularly at global conferences and is a frequent contributor of articles in professional and business publications.

About Galvanize

Galvanize builds award-winning, cloud-based security, risk management, compliance, and audit software to drive change in some of the world's largest organizations. We're on a mission to unite and strengthen individuals and entire organizations through the integrated HighBond software platform. With more than 7,000 customer organizations in 140 countries, Galvanize is connecting teams in 60% of the Fortune 1,000; 72% of the S&P 500; and hundreds of government organizations, banks, manufacturers, and healthcare organizations.

Whether these professionals are managing threats, assessing risk, measuring controls, monitoring compliance, or expanding assurance coverage, HighBond automates manual tasks, blends organization-wide data, and broadcasts it in easy-to-share dashboards and reports. But we don't just make technology—we provide tools that inspire individuals to achieve great things and do heroic work in the process.

wegalvanize.com