IDC Government Insights

Best Practices: A ProveIT Case Study — Washington State Implements Business Analytics Tools and Recovers Millions in Government Funds

IDC Government Insights: United States Government Infrastructure Optimization

BEST PRACTICES #GI228992

Shawn P. McCarthy

Worldwide Headquarters: 7600 Leesburg Pike, East Building, Suite 310, Falls Church, VA 22043, USA P.703.485.8300 F.703.485.8301
www.idc-gi.com

IDC GOVERNMENT INSIGHTS OPINION

In tight budget times, government agencies need to be able to promise improved business outcomes and a positive return on investment (ROI) — if they want funding for new IT solutions. One investment that seems to pay consistently high dividends is a system that can help managers discover and recover money that's owed to them. A solution developed by the Fraud Prevention and Compliance group within the Washington State Department of Labor and Industries is one such example. The department faced a dilemma three years ago when it needed to analyze multiple data sets — as it worked to better detect possible instances of fraud in its workers' compensation program. We believe that this data integration example can provide several "best practices" for other offices that seek a similar fraud analysis solution. In detail:

- Because fraud investigators required access to data that resided on multiple government systems, they first build a centralized review office and then a centralized data mart capable of collecting data from multiple other departments and databases.
- Because the group needed to analyze large data in new ways, it selected a complex (but commercial off-the-shelf [COTS]) statistical analysis package specifically developed for fraud analysis. The solution contains fraud analysis tools and the ability to look for patterns that highlight unusual claims activity, policy holder activity that doesn't match up to known patterns, and predictive analysis based on known associations and networks of individuals.
- The centralized fraud detection system is on track to achieve a positive ROI in less than two years. Ultimately, it's on track to recover millions of dollars each year. In the process, it's also boosting compliance and helping the state find new ways to share and analyze data across multiple departments.

TABLE OF CONTENTS

LIST OF FIGURES

IN THIS STUDY

Each year, IDC Government Insights publishes a series of "ProveIT" case studies. In these documents, IDC Government Insights analysts take a look at a specific government business need and then analyze a successful IT approach that has been used to answer that need. We specifically focus on business issues and needs, such as return on investment, risk, transformation, and the level of innovation involved in the particular solution.

This ProveIT case study looks at how business analytics can be used as part of a government fraud detection effort. This specific example highlights the Washington State Department of Labor and Industries, and how the department used analytics software and a new integrated system to improve fraud detection and recover millions of dollars for the state. The chosen solution also helped the department cut some expenses, streamline business operations and workflow, and improve overall efficiency.

The approach taken by the department can be considered a set of best practices for organizations that have a similar need to restructure their fraud analysis and the way fraud-related information is collected and shared.

Methodology

This ProveIT case study highlighted in this document is based on interviews with Carl Hammersburg, manager of Fraud Prevention and Compliance at the Washington State Department of Labor and Industries. We also reviewed additional information provided by the SAS Institute and culled details from reports published directly by the Washington State Department of Labor and Industries.

All IDC Government Insights ProveIT case studies follow a prescribed method, which is outlined in *ProveIT Case Study Methodology* (IDC Government Insights #GI217422, March 2009).

All IDC Government Insights ProveIT case studies follow a prescribed method, which is outlined in *ProveIT Case Study Methodology* (IDC Government Insights #GI217422, March 2009).

This document is divided into several sections. The relevant business issues and performance metrics, which make up the foundation of the ProveIT analysis, are addressed in the following sections:

- The Return on Investment Analysis section looks at both the operational costs and the government business value (service to citizens) achieved via the chosen solution.
- The Risk Analysis section examines the situational complexity associated with this project and possible stumbling blocks. We look at both technical risk and situational issues which could have

a negative impact on the organization if complications ensue during the project.

- The Transformation section covers how the project impacts the delivery of services that are core to the department's mission, business processes, operational funding, and security requirements. It also highlights some lessons learned, plus a look back at how things might have been done differently.

- The Innovation section looks at how creative the solution is and how best practices related to this solution might be approached — by other organizations — for scalability and repeatability.

SITUATION OVERVIEW

The state of Washington manages its own workers' compensation program. This type of program, common throughout the United States, is a form of insurance which provides wage replacement and covers medical expenses for employees who are injured while working. Employers pay into the state program, based on numbers of employees and other factors related to job risk.

Virtually every working person in the state is covered by the program, with the exception of approximately 400 large corporations that run their own workers' compensation program.

The Fraud Prevention and Compliance group within the Washington State Department of Labor and Industries is charged with preventing abuse or fraud within the state's workers' compensation program. The group has about 250 staffers dedicated to handling employer compliance, claims investigations, and various types of audits and collection issues.

The Fraud Prevention and Compliance group handles multiple duties. For example, the office:

- Conducts more than 5,800 audits yearly to ensure employer compliant reporting and payment

- Performs nearly 5,800 investigations to prevent abuse or fraudulent payments to workers who were not injured, not injured on the job, or may have returned to work while claiming they are still disabled

- Audits more than 220 medical providers to ensure proper billing for procedures performed

- Collects outstanding debts for all overpayments, audits, fines, and past due premiums on more than 20,000 people and firms each year

About six years ago, the Department of Labor and Industries estimated that it was losing more than $100 million per year because of various types of workers' compensation fraud. But analyzing exactly where the shortfalls were occurring was a very complex task. Like many organizations tasked with processing reports and claims, the department found it challenging to detect fraud patterns when dealing with a large volume of information.

Managers addressed the issue with a two-pronged approach: they decided to centralize data resources and fraud detection efforts and they sought technical solutions to help better analyze the available data, with the goal of boosting the organization's revenue recovery rate.

Managers also hoped to improve data integration and the overall efficiency of their business process related to collection of premiums and the payment of claims.

Business Needs

In response to the situation outlined previously, the Washington State Department of Labor and Industries initiated an effort to identify all gaps in its detection and its management of possible workers' compensation fraud. The first challenge was that various pieces of the workers' compensation program, and related data, were stuck in different government divisions. The department elected to create a central division with its own separate chain of command. This office, known as Fraud Prevention and Compliance, worked to improve internal fraud detection functions and made decisions on how and when to pass leads (and which leads) to investigators.

The Department of Labor and Industries faces some unique challenges because of state laws. For example, the department is responsible for paying a workman's compensation claims, even when no premiums have been received from an employer. At the same time, Washington, like many states, has an "underground economy" of sorts that motivates some employers to underreport the number of workers they employ — which can artificially decrease the premiums they owe.

Pressure for reforming this situation was not only internal. Policy holders (meaning employers that were using the system in the correct way) asked the office to find a way to make premiums and coverage fairer for all.

The centralized division currently has a staff of 251 people, out of which 75 are totally focused on employer premium audit and 62 are field auditors. Business experts do the initial screenings and send out the investigation leads.

Before the division was centralized, when auditors received the leads, their investigations uncovered a significant compliance or fraud issue

just 50% of the time. That's because they were not always able to identify and target the cases that were most likely to involve fraud or abuse, and because they didn't always have easy access to data that might allow them to solidify their cases.

Feedback from stakeholders of the group indicated that many had concerns about fraud, the group's ability to detect fraud, and the group's ability to channel investigators to the most promising leads. There also was concern that the right tools might not be in place to detect all of the information that could help uncover fraudulent activities.

The business need, in a nutshell, was that the office needed to be centralized in order for workers to conduct their investigations in a coordinated way. The initial centralization effort and internal detection improvements through computerized crossmatches moved the needle from 50% in 2004 to 60% by 2009, meaning that the auditors started uncovering more real and actionable issues when they received new leads.

But during its investigations, the centralized team realized that it was only finding the tip of the iceberg when it came to uncovering fraud. It quickly realized that employees had a dire need for a new system that could improve staff efficiency while targeting the cases that seemed most likely to result in a positive outcome.

Tips about suspicious claims and possible fraud can come via other departments. To process such tips, the centralized division discovered that its workers had to log into as many as 12 systems when looking for data and possible leads. The heavily manual process also involved sets of paperwork and other internal resources.

The division needed a way to integrate the multiple data sets available from multiple programs and agencies, and it needed the right tools to scan that data for inconsistencies and possible leads for investigators.

Management Challenges

According to Hammersburg, the group promptly sought to automate the fraud analysis process and improve related business analytics. "We talked with many solution providers," Hammersburg said, "most were heavily focused on identity resolution, but they did not offer the other needed analytics."

The group came up with a list of what it needed for a new fraud analysis system and prepared a budget proposal for submission to Washington's governor and legislature. Project costs were estimated at $8 million and included a plan to buy some of the necessary software while building other parts of the solution itself. Over the years, the

group had talked with multiple vendors and did not find a full solution available that addressed all of its needs, especially fraud targeting.

Receiving the go-ahead from the legislature in May 2009, the team issued a request for proposal (RFP). In Washington State, vendors can sign up to automatically receive a notification when such requests are issued.

The RFP for the new fraud detection system was issued in July 2009. Based on that RFP, Hammersburg said the group received five bids. One came from the SAS Institute and others came from IBM Corp., Ascentium, Revenue Solutions Inc. (RSI), and Valen Technologies. Two of the proposals indicated that they would use SAS software as part of their solution.

At that time, the team didn't know much about the SAS Institute but did know that the company's analytics software was in use elsewhere in Washington state offices, mostly by workers who deal with statistics and other data.

After evaluating the proposals and learning more about available software solutions, the team changed its focus. It realized it might not have to develop its own customized portions of the fraud detection system. It ended up selecting SAS as the main provider of the solution in September 2009. Hammersburg said the selection was made because of the company's price and specific capabilities.

Planners met with the SAS team to set final requirements in November 2009 and began building the system in January 2010. It took a little over a year to first implementation at the desktop level in December 2010. The remaining phases rolled out during spring 2011.

Hammersburg added that his group knew, when embarking on the project, that the SAS proposal would require a bit more system integration than other proposed solutions, but that was acceptable under the project's goals and budget. The solution also gave them real-time access to multiple data sources, which was an added bonus. Despite needing some systems integration, the team worked to keep the project as standard as possible, to minimize custom coding.

One bit of needed integration was to interface with IT systems of state tax and unemployment agencies, as well as the IRS. This was the most complex portion of the project. For that piece and other in-house technical design work and business design consulting, the team selected Brewer Consulting Services of Olympia, Washington, a small woman-owned business.

Funding

With its $8 million budget set, the group spent $1.6 million for SAS software and services. It also spent $700,000 in new hardware and equipment. The full project, including other systems integration and IT services, cost about $5 million, including two new permanent employees.

That means the full project came in significantly under the original $8 million budget.

The Washington State government has a two-year budget cycle. Funds for this project became available July 1, 2009. It is designated as a two-year project with a solid end date of June 30, 2011. All decisions must be made and money must be spent within that time frame. The timeline called for the project to be completed by May 30, 2011.

The Solution

Data from over a dozen different internal sources, plus two external sources, is imported into a new centralized data mart. Local data is refreshed daily. Some claims-related data is refreshed in near real time. Besides the database, the group's next step was to use the SAS software to implement a fraud framework, taking a blended approach that combined rules-based predictive modeling and data analytics.

Enterprise data and rules resources include details on specific policies, claims, revenue, filed tax documents, unemployment claims, and safety inspection reports (which often include details on workers and other things noted at the work site during the inspection). Also included are external tips from people who know or suspect that an employer might be involved in fraudulent activity. The system allows staffers to integrate leads and tips with analytics and scoring results, to see if additional investigation is warranted.

From their desktops, fraud investigators can now detect fraud issues, check compliance, note anomalies, look for connections, and identify leads for investigators. In the process, they often are able to identify specific people who may be involved in a case and are able to sort data and results by industry, geography, time period, type of issue, known connections of the people involved, and more.

One very important way of sorting the information is to identify the highest priority leads — based on screening for specific details like amount owed, numbers of people involved, or people with a history of other offences.

Such rules can quickly identify suspected fraudulent behaviors. These tend to fall into the following categories:

- **Known patterns,** such as notes of a safety inspection that identified workers on a site but in a quarter when no premiums were paid by the employer (Or, it might call out a claim that was filed but that no risk class or rate was identified for that employer.)

- **Unknown patterns,** where anomalies are detected, but the specifics of those anomalies still need to be identified (These can include things like noticing that an employer's revenue increased at a time when the number of the employer's workers decreased, or when an employer reports worker hours within a specific risk class — but only in quarters when an employee also had a claim filing in that risk class.)

- **Detection via predictive models,** which are developed from complex patterns comparing known fraud cases with new issues (These can identify things like similar premium-filing patterns or similar claim-filing patterns.)

- **Detection via associative link patterns,** including social network analysis, by which investigators can uncover associative links, such as interactions with known fraudsters or unusual patterns for employees who work for specific employers

Near the beginning of the project, the group drilled through several years of data and audits, looking for common patterns. Examples include things like work hours versus employee wages, which it could compare to look for anomalies. The group also discovered some unexpected trends, such as missing fields, which often indicate underreporting. The group learned, over time, which trends were real leads for fraud investigators and which ones paid off while others might not.

Looking across multiple categories, the organization used the SAS software to develop employer profiles and fraud scores. It could compare employees with peers and industry profiles to see where they fit versus the full group.

By reviewing associations, common employers, common coworkers, and more, investigators can detect links between current investigations and previous known frauds. Such links can be made through names, relationships, shared addresses, shared phone numbers, and more. Investigators can learn about other parties which haven't scored high for fraud yet but which seem to be following a specific pattern or interacting with known fraudulent entities, which might eventually lead toward suspicious behaviors. They also are able to identify the growth of certain networks of suspicious individuals over time.

As investigators use the fraud detection system, a feedback loop gives reviewers the ability to adjust the weighting for some data elements,

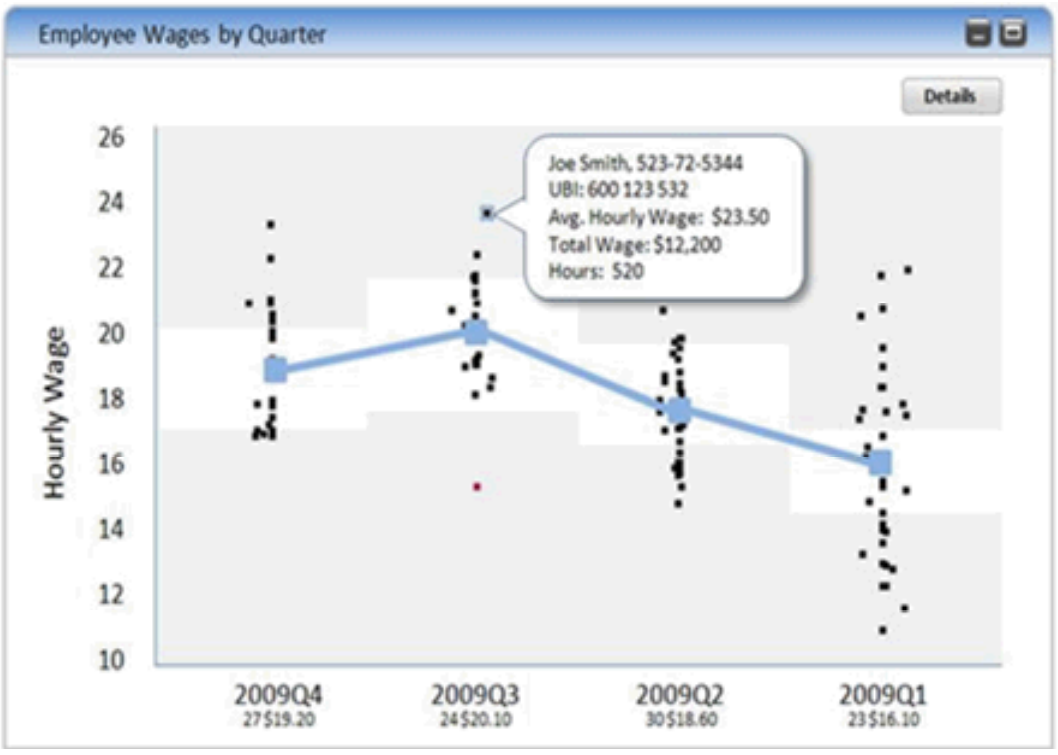
allowing them to improve, over time, the accuracy of the way they apply certain measurements and successfully detected fraud.

Figure 1 shows one way that the system is able to display data related to average hourly wages. It's a way to compare worker wages over time. In Figure 1, the blue line indicates the overall average wage for a specific job category and the white boxes show the expected range for such wages. Outliers show wages that seem high or low compared with others. Each dot can be selected to show additional information. The bottom of Figure 1 shows specific reporting quarters, number of employee wages reported, and average amounts.

Thresholds can be set to highlight one or more issues. Outliers can be a good indication that total hours or other information for the company has been underreported or misrepresented.

FIGURE 1

Data Display: Outliers Within Data Samples Immediately Noticeable



Source: Washington State Department of Labor and Industries, 2011

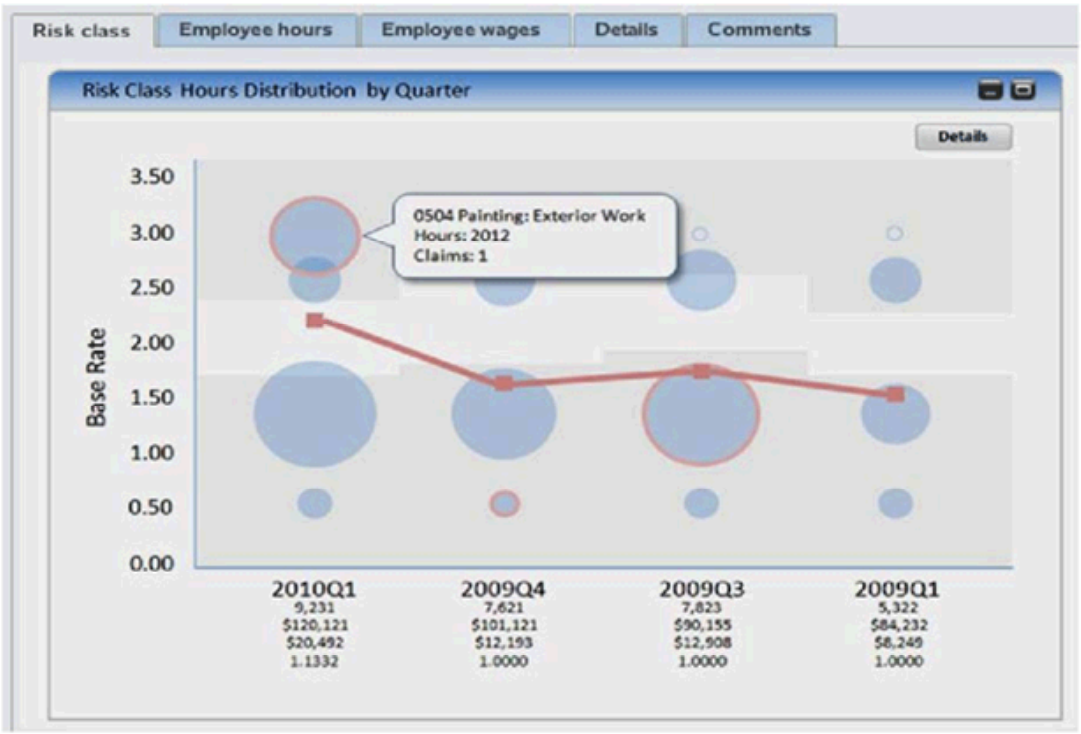
Figure 2 shows another way that data can be displayed to highlight possible suspicious patterns. In this case, Figure 2 provides details

related to a specific painting company. It shows that company's reporting by risk classification over time (weighted averages). In this view, less expensive risk classes appear lower in the display. More expensive classes are shown higher in the display. Bubble size is based on the amount of reporting for each class for a given quarter. (If the bubble is small with no shading, the company reported no hours in that risk class for that quarter.)

This view shows that the firm in question filed a claim for the first quarter of 2010. It also shows that the firm reported 2,012 hours worked in the most expensive risk class, which is also where the injury was reported. This is not a problem by itself, but this data view shows that zero hours were reported in the most expensive risk class for all other quarters shown. Based on set rules in the system, this is identified by the system as suspicious. An investigator might elect to look closer at this case because of the data pattern identified by the system.

FIGURE 2

Data Display: Highlighting Suspicious Patterns for Injury Claims



Source: State of Washington Department of Labor and Industries, 2011

Return on Investment Analysis

The centralized fraud detection is on its way to experiencing a positive return on investment in under two years. This ROI can be charted in several ways, including increased revenue, faster processing time, improved employee morale, and the discovery of new ways to leverage the information uncovered by the fraud detection solution.

The initial improvement started three years ago. As reported previously, investigators were used to uncovering a true fraud issue just 50% of the time when they investigated a possible fraud issue. Centralizing the resource pushed that needle from 50% to 60%, with a recovery average of $8,000 per audit.

Once the new fraud detection software and associated system were installed in 20l0, the group pushed that needle to 73%, and Hammersburg believes it can hit 80% by the end of 2011. It also is recovering more than $10,000 per investigation.

With just under $5 million invested so far, the organization expects to identify more than $8.3 million more in premium audits each year. Hard collections will exceed an additional $3.3 million per year — compared with previous annual collection levels. That will lead to a positive ROI in under two years.

A primary focus of the project is uncovering employers that are completely unregistered for workers' compensation and bringing them into compliance. The organization expects this area to increase over 2010 baseline by 20% by June 2012 and 40% by June 2013.

With early leads looking more positive than originally expected, Hammersburg's new goal is a $5 million return by June 2012, increasing over time, with a 20:1 return for the investment within five to seven years.

Another benefit: Initial screening time for applications has dropped by 80% (from 3 to 4 hours down to 15 minutes).

Plans are in development to integrate leads with broader business areas across multiple government groups. Information gleaned in the fraud detection unit might end up increasing compliance and collections in other business areas.

The group has already secured funding for the first expansion of the system, beginning in July 2011. That expansion will focus on the underground economy that exists within the construction industry and the broad compliance issues that often are present there — contractor registration, wage and hour, and prevailing wage enforcement as well as workers' compensation. It will add additional data sources, such as construction permits and prevailing wage intents and affidavits. The

targeting model will also shift from being focused on just what employer to look at to specific jobsite activity that should be inspected in person by our field inspectors.

Hammersburg reports that workers in the group seem satisfied with the new system. They are able to find the data they need without having to contact multiple other information owners across departments. They also are able to uncover nearly all the information they need when making important decisions, and they can now notice trends that they may not have been able to detect before.

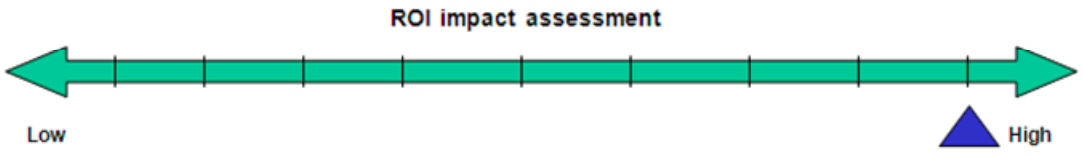
Right now the system is identifying more issues than the staff can handle. So thresholds have been set so that investigators can first handle the biggest targets with the most likely payoffs. Right now they are routing some cases to other staffers (underwriters, etc.) for help with the investigations. They've found that this helps those workers understand fraud and what to look for.

But, Hammersburg added, "the results actually are constrained by our staffing limitations — more than the targeting capabilities." Based on its success rates so far, he said the group is looking into adding additional staffers to help with the revenue recovery effort. He also admits that the improved collection efforts, while substantial, won't continue forever. One result of improved enforcement is also improved compliance in the future. At some point, there should be less fraud simply because the government has improved at catching fraud. The numbers will eventually flatten out, but that still means improved long-term revenue for the department.

Few of our ProveIT case studies are awarded an ROI impact rating at the highest level. But Figure 3 shows our assessment of the ROI impact for the department's strategy. In this case, the impact is high because of the ratio of investment to savings and also because the group was able to gain significant improvements to overall business processes for its fraud detection and collection efforts.

FIGURE 3

ROI Impact: IT Investments to Improve Fraud Prevention and Compliance Systems



Source: IDC Government Insights, 2011

Risk Analysis

This project had a fairly low technical risk. The department did not replace existing systems. It installed a new system with imported data from the older systems. Thus there was very little risk that the existing business process within the department would fail. Planners were able to get the new system up and running without affecting the day-to-day operations of the other systems.

The SAS software resides in a Microsoft.NET environment. Contract analytics/modelers worked well with their team, and only minor issues arose during the system design.

The only major modifications were to integrate with existing audit system and the state's tax system. But these integrations were done using existing APIs and links — which already were supported by those other systems. No major adjustments were needed to the other software, and only minor configuration changes were needed for the server hardware. Based on the amount of data now collected, the group also will need to add some servers and storage.

Technical Details on Data Merging

Hammersburg said the group knew up front that data quality and matching would require significant work — as part of setting up the data mart and doing the extract, transform, and load (ETL) work as part of moving the information into the data mart. In some cases, it was known that a particular agency was much more reliable for quality of a particular data field. Working through those types of details up front allowed for multiple approaches when setting rules for the data mart, identity analytics, and population of the user interface.

An example of an override approach to the data mart — based on quality — is the Federal Employer Identification Number (FEIN), a critical data point to match state data with IRS information. While the Department of Labor and Industries had that number on many firms, it did not always have the information or have it accurate. The State Revenue Department always had that field and high-quality information. As a result, the implementation is set to populate the FEIN field by matching with the State Revenue Department off of state indicators first, then use its information as a primary source for the FEIN.

In other cases, the matter isn't as clear cut. There may not just be a right or wrong answer. There may be multiple correct answers, such as addresses. For those situations, the data mart populates from *all* the fields available, finds the highest or most likely matches, and presents those first but allows viewing from the additional sources. When doing identity resolution, it also presents "near" matches that screening staff can choose to combine in the primary identity profile as appropriate.

System developers did experience some lag at the beginning related to integrating the multiple data sources, but those issues were worked out. Because this work was being done in a state government office, SAS employees needed background checks before they were allowed access to the facility in order to design and build the system. Citrix's software was used to enable remote connections for SAS workers based in North Carolina.

Hammersburg said it's important, when undertaking this sort of data integration project, to find a vendor that is responsive to the government's needs. He said the integration team reacted to specific project management issues raised by his organization — an early project manager was not well suited for the organization's requirements and was replaced by SAS. Also, the group encountered some complications with the project's scope, based on timeline requirements. The contractors added resources when the need arose, at no additional cost.

While the technical aspects for this project were fairly low risk, there was a low-to-moderate risk associated with changes to the group's business processes.

From a workflow standpoint, there were moderate business process changes related to underwriting classifications, and changes also were made to the way the review staff reviews data and identifies problems. This required training on how to use the new system and how to adjust the workflow based on how employees use the system.

Despite the changes, staff feedback was positive because many of the staffers had been asking for a solution that would provide this level of data analysis. Hammersburg said other employees in the department have asked for access to the SAS desktop applications so that they too will have access to the data and the analysis tools.

Figure 4 shows our assessment of risk impact. If we were to only measure risk, then the arrow would be a bit closer to the low end of the scale. Since this was a newly installed system, it did not affect business as usually until the system was up and running and working. But the organization also had to manage project risk, risk a substantial capital investment, and migrate workers away from an older way of doing business. Because of these other issues, we have to rate the risk for this project in the middle. It wasn't high risk, but it still included some organizational and capital risks.

FIGURE 4

Risk Impact of Changes to Fraud Prevention and Compliance Systems

Source: IDC Government Insights, 2011

Transformation

This project essentially transformed the way the fraud detection group handled its investigations. But this change was not meant to significantly transform the full business process of the Department of Labor and Industries. "We just took the data from other places around the department," said Hammersburg, "and we were able to show what we could do with it." He added that his office "did have to renegotiate some contracts with internal partners." The challenge was higher when dealing with data-sharing contracts with other agencies, especially when federal as well as state laws apply to the information. Using both private contractors and people located outside of the group were barriers that required some intense work to manage when external partners identified risk.

A larger transformation occurred in the way data flows into the fraud group, and how that data is analyzed after it arrived. The new fraud analysis system gave employees a new platform from which to conduct their business, and it refocused their efforts in a way that proved much more productive for the full organization.

This transformation essentially moves the organization from detecting fraud after the fact (and working toward recouping payments) to being a more proactive organization that's capable of quickly detecting fraud, stopping it, and preventing future fraud from happening. And, rather than dealing mostly with individuals or companies, it now is able to detect fraud rings, both in small groups and as components of larger criminal organizations.

These changes also have transformed the fraud detection staff from a group of people who spent much of their time chasing data sources to a group that now focuses most of its time on enforcement. And staffers are able to better leverage time spent by shepherding their efforts toward cases with the best potential payoff for their labors.

Fraud against many government agencies, including the Washington State Department of Labor and Industries, is huge. But such fraud

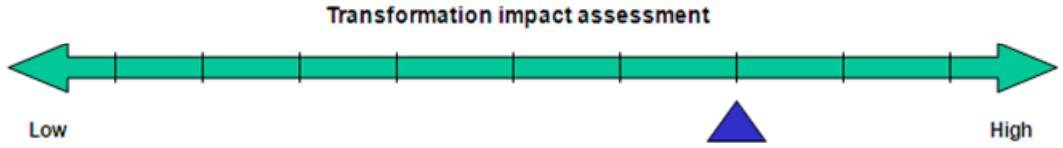
often happens over a long period of time, with multiple individual fraud transactions. This type of system allows for faster comparison of details in a way that can be used to detect obscure anomalies. This not only has improved enforcement efforts but can help prevent other legally compliant participants from dropping out of the system because of the frustration that might be caused when they see other companies and workers "getting away with" noncompliance.

From a pure technology standpoint, a significant transformation also occurred. As mentioned previously, a new system and a data mart were created for the centralized facility. SAS comes on its own dedicated server (Microsoft).

Figure 5 shows our assessment of the transformational impact of these changes. If we were only to measure the transformation of how fraud is detected and handled, then the assessment would be near the top because the solution was indeed transformative. But we also have to consider the full business process that's involved in collecting and analyzing relevant data. System planners built a centralized data mart capable of collecting data from multiple other departments and databases because all of those other databases were outside their direct control. Thus, further enterprisewide transformation of where data lives and how it is integrated could even further streamline operations and improve specific business functions. But this is obviously a larger project that needs to involve multiple other state organizations.

FIGURE 5

Transformation Impact of Information System Updates Related to Fraud Detection

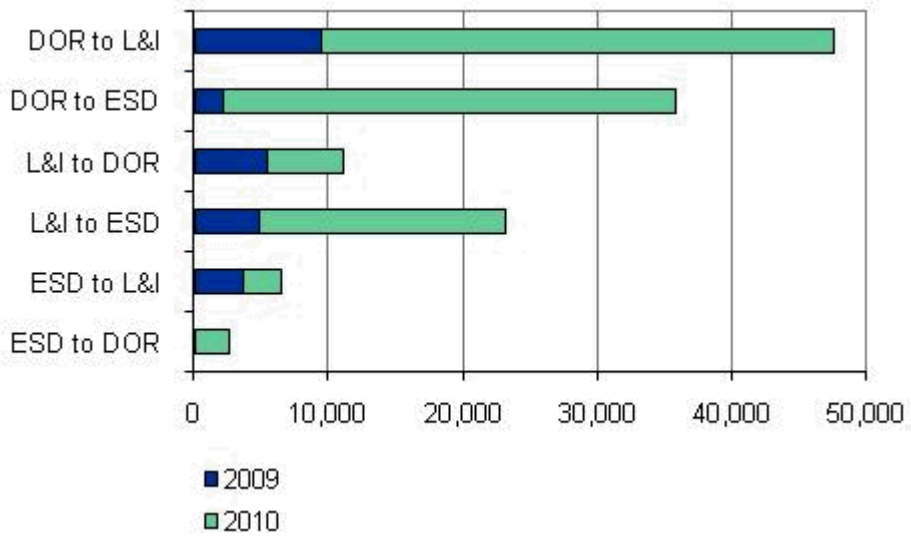


Source: IDC Government Insights, 2011

Figure 6 shows how the new system helped improve the way data is electronically exchanged between state agencies. Between 2009 and 2010, the number of electronic files exchanged between the Department of Revenue, the Employment Security Department (Unemployment), and the Department of Labor and Industries in Washington jumped from under 26,000 annually to over 101,000 annually.

FIGURE 6

Cross-Department Referrals via Electronic Data File Transfer, 2009 and 2010



Source: Washington State Department of Labor and Industries, 2011

Centralizing the fraud detection staff, and its data resources, was the first step in a much bigger transformation effort. The addition of the SAS fraud detection tools significantly changed the way the organization conducts business, and the payoff has been substantial.

Innovation

It's fair to say that this solution is significantly innovative compared with what the department had in place. It's even innovative compared with the initial plan of the group to centralize its resources and build its own system. The server/software/integration solution chosen by the team brings a new set of tools to its fraud detection efforts, giving employees the type of data views they wanted. It also gives the employees the ability to integrate new data sources and customize their data views.

The group has found value beyond the original anticipated scope of the project. It is able to identify a higher percentage of productive cases to investigate, and it has found a higher percentage of recoverable funds. And from a technical standpoint, work done to help extract, transform, and load multiple data sources into a single data mart provides a workable model for future efforts to merge data and systems across the enterprise.

One of the final pieces of the project will be integration with the state's audit system, which will give auditors a distinctive view of how funds are being recovered and channeled back to the state.

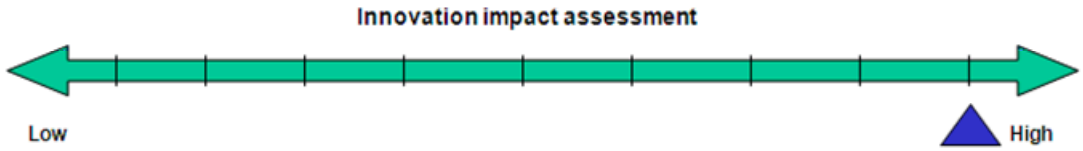
Fraud recovery often involves collecting data from multiple sources, and because data elements can vary considerably, it's quite common for government organizations to choose internal development of a highly customized system. Thus the choice made by the Department of Labor and Industries was creative because it went with a commercial off-the-shelf solution while choosing to put its customization efforts into shared system connections and a shared data mart, which gives it a more powerful and flexible data integration solution for the long term.

The Best Practices section outlines some of the best practices related to the state's fraud prevention solution. We consider several of these practices to be innovative and worth adoption by other organizations looking for a similar solution.

Figure 7 shows our assessment of the innovation impact of these changes. In this case, the assessment is very high because the new process significantly changed both the way fraud is detected and how information related to fraud is analyzed. While much of the innovative credit goes to the SAS Institute for developing the fraud analysis solution, the Department of Labor and Industries is using the solution in an innovative way, integrating significantly different data sources to help triangulate instances of fraud.

FIGURE 7

Innovation Impact of Changes to Fraud Prevention and Compliance Systems



Source: IDC Government Insights, 2011

THE BEST PRACTICES

One of the Department of Labor and Industries' decisions that we consider to be a best practice for other organizations is its choice to build a central data mart that imports data from other databases. For a new project such as this one, this was wise from a political perspective because it does not require any current data "owner" to give up control

of its data. The data owner is simply sharing it now, via an automated solution that imports relevant data into the central data mart.

Having control over one's own data mart also allows the data to be filtered and augmented if needed. For example, data field names can be adjusted or certain fields can be stripped out if they are redundant.

Keep in mind that simple rules-based fraud detection systems may not be powerful enough to detect more complex patterns, which could point to highly possible fraud activity. That's why the fraud unit's centralized fraud detection system proved more valuable for detecting anomalies. For example, a company reported 2,012 hours worked in a specific risk class and also filed a claim in that risk class (refer back to Figure 2). A basic rules engine might consider this acceptable, while a more extensive pattern analysis can detect inconsistencies across multiple quarters.

Other best practices include:

- Tracking results to refine future fraud research by identifying key patterns that have proven successful in highlighting fraud activity
- Providing information to management and stakeholders across other departments to help develop a sense of teamwork and informed decision making
- Building public awareness campaign to highlight the state's fraud-fighting activities and to encourage compliance

FUTURE OUTLOOK

The next phase of expansion will focus on the underground economy that exists within the construction industry and the broad compliance issues that often are present there — contractor registration, wage and hour, and prevailing wage enforcement as well as workers' compensation. It will add additional data sources, such as construction permits and prevailing wage intents and affidavits. The targeting model will also shift from being focused on just what employer to look at to specific jobsite activity that should be inspected in person by our field inspectors.

Additionally, that phase will stand up a second iteration of the SAS Fraud Framework outside of the highly secured environment containing IRS data. That iteration will also be scaled for a much larger user group, making it available at a desktop level to all staff in premium audit, underwriting, and account management and collections.

The department continues to analyze additional expansion options in the future, including safety inspection targeting and claims fraud targeting.

ESSENTIAL GUIDANCE

Actions to Consider

Advice to those considering this type of fraud detection or other business and data analytics solution is as follows:

- Set the project up through a deliverables-based contract. In this case, the contractor had to add resources to finish a job on time, and they did so with no additional cost to the state.
- Do a detailed requirements analysis up front. This is an advanced tool. Understand what it can do. Understand what you need it to do and set the project plan accordingly.
- Seek the right people for the right project and don't limit your organization's long-term viewpoint. Consider who can benefit from viewing business analytics information and visualize ways the system can expand over time to take on the significant effort of targeting data for analysis related to other business processes.
- Ensure that business process experts are deeply embedded in the process for modeling and analysis. They will balance the expertise of modeling experts who are not experts in a given agency's experience and legal constraints.

Lessons Learned

- Predictive modeling is an advanced approach to targeting. It brings huge value but may not reflect all risk appropriately if past results were limited or skewed. Always do a "sniff test" when working through iterative models.
- Bringing together data from many sources is challenging and will require significant time out of the full project timeline. Learn which data sources are the most reliable, and define how they override similar fields from other sources.
- Keep close track of project timelines and where development is at on any of them. Find a balance of when to push back on internal and external teams that keeps the relationships in place, but ensures you can meet deadlines, especially if they are legally mandated.

LEARN MORE

Related Research

- *What Does the President's Cybersecurity Plan Mean for Federal Agencies?* (IDC Government Insights #lcUS22839411, May 2011)
- *U.S. State and Local Government IT Spending Guide, Version 2, 2009–2014* (IDC Government Insights #GI227646, March 2011)
- *U.S. Federal Government IT Spending Guide, Version 2, 2009–2014* (IDC Government Insights #GI227656, March 2011)
- *SAS Renews Its Focus on Government Solutions* (IDC Government Insights #lcUS22745611, March 2011)
- *Oracle Pitches IT Modernization and Advanced Integration to Help Reinvigorate the Public Sector* (IDC Government Insights #lcUS22716011, February 2011)
- *Perspective: IT Spending in the 2012 U.S. Federal Budget — Details by Agency* (IDC Government Insights #GI227023, February 2011)
- *Vendor Assessment: Top Federal Government IT Vendors by Agency, 2009* (IDC Government Insights #GI226808, February 2011)
- *Vendor Assessment: Top 25 IT Services Vendors Tell a Larger Story — Government Datacenter Consolidation* (IDC Government Insights #GI226454, January 2011)

Synopsis

This IDC Government Insights report takes a look at how business analytics can be used as part of a government fraud detection effort. One IT investment that often pays high dividends for government agencies is a system that can help them discover and recover money that's owed to them. A solution developed by the Fraud Prevention and Compliance group within the Washington State Department of Labor and Industries helped that office recover millions of dollars, achieving a positive ROI for the project in under two years while decreasing screening time of some applications by 80%.

"The fraud framework takes a blended approach," says Shawn P. McCarthy, research director at IDC Government Insights. "It combines rules-based predictive modeling and data analytics in an innovative way, allowing investigators to quickly highlight suspicious activity. This allows them to effectively and efficiently target their recovery efforts."

