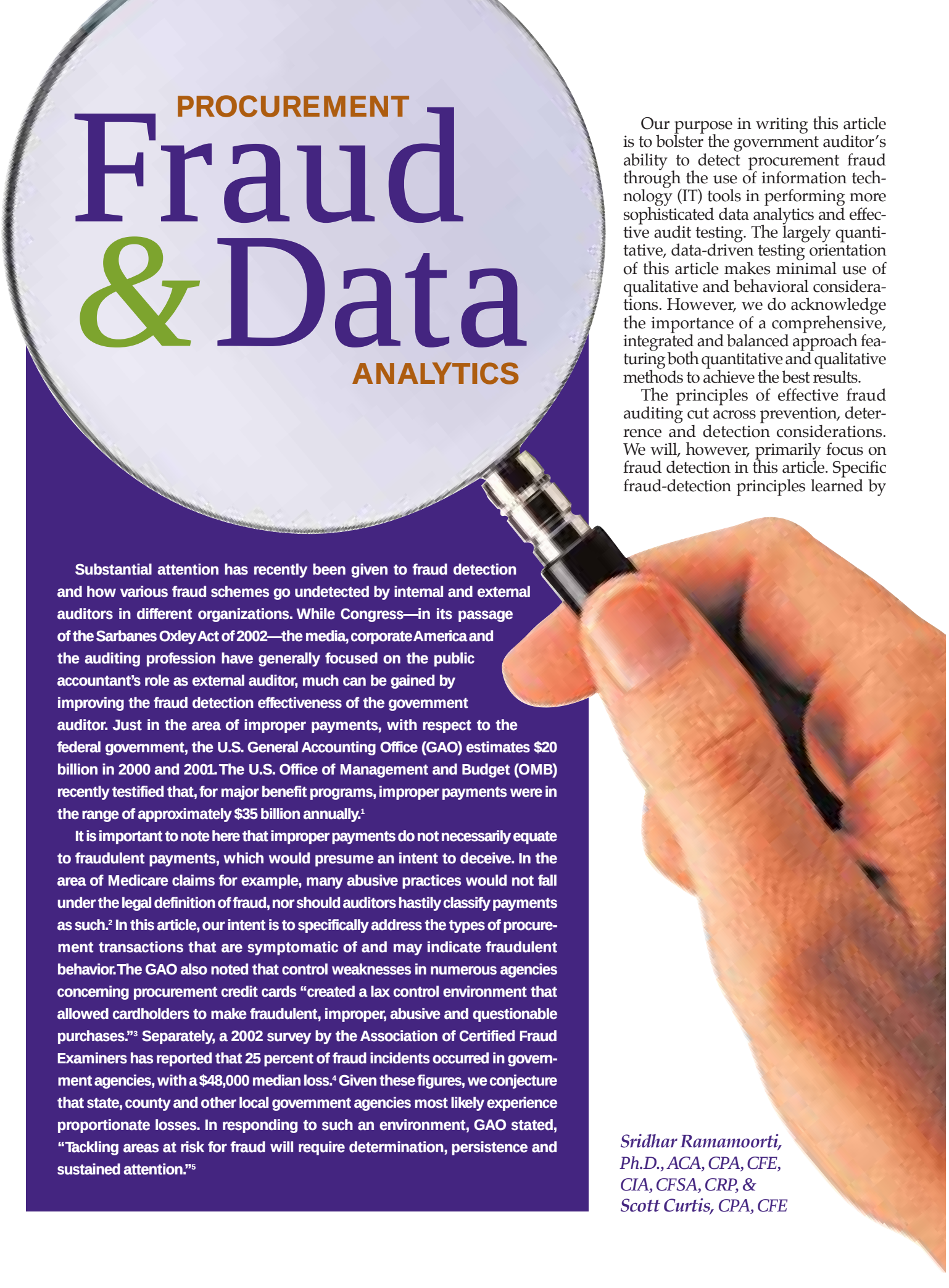
12-1-2003

Procurement Fraud & Data Analytics

Sridhar Ramamoorti
University of Dayton, sramamoorti1@udayton.edu

Scott Curtis

PROCUREMENT Fraud & Data ANALYTICS



Sridhar Ramamoorti, Ph.D., ACA, CPA, CFE, CIA, CFSA, CRP, &
Scott Curtis, CPA, CFE

Substantial attention has recently been given to fraud detection and how various fraud schemes go undetected by internal and external auditors in different organizations. While Congress—in its passage of the Sarbanes Oxley Act of 2002—the media, corporate America and the auditing profession have generally focused on the public accountant's role as external auditor, much can be gained by improving the fraud detection effectiveness of the government auditor. Just in the area of improper payments, with respect to the federal government, the U.S. General Accounting Office (GAO) estimates $20 billion in 2000 and 2001. The U.S. Office of Management and Budget (OMB) recently testified that, for major benefit programs, improper payments were in the range of approximately $35 billion annually.[1]

It is important to note here that improper payments do not necessarily equate to fraudulent payments, which would presume an intent to deceive. In the area of Medicare claims for example, many abusive practices would not fall under the legal definition of fraud, nor should auditors hastily classify payments as such.[2] In this article, our intent is to specifically address the types of procurement transactions that are symptomatic of and may indicate fraudulent behavior. The GAO also noted that control weaknesses in numerous agencies concerning procurement credit cards "created a lax control environment that allowed cardholders to make fraudulent, improper, abusive and questionable purchases."[3] Separately, a 2002 survey by the Association of Certified Fraud Examiners has reported that 25 percent of fraud incidents occurred in government agencies, with a $48,000 median loss.[4] Given these figures, we conjecture that state, county and other local government agencies most likely experience proportionate losses. In responding to such an environment, GAO stated, "Tackling areas at risk for fraud will require determination, persistence and sustained attention."[5]

Our purpose in writing this article is to bolster the government auditor's ability to detect procurement fraud through the use of information technology (IT) tools in performing more sophisticated data analytics and effective audit testing. The largely quantitative, data-driven testing orientation of this article makes minimal use of qualitative and behavioral considerations. However, we do acknowledge the importance of a comprehensive, integrated and balanced approach featuring both quantitative and qualitative methods to achieve the best results.

The principles of effective fraud auditing cut across prevention, deterrence and detection considerations. We will, however, primarily focus on fraud detection in this article. Specific fraud-detection principles learned by

experience will demonstrate universal application to a variety of individual situations. We hope that such a principle-based approach will provide greater insight and benefits in the long run, as the ability to adapt and adjust to a changing environment will serve government auditors in any agency much more than simply following a standard checklist. The government auditor should customize the application of general fraud detection principles to specific facts and circumstances and use sound professional judgment. Procurement fraud detection tests may help identify fraudulent activity but also inefficiencies, waste and abuse. Although the size of the agency will likely influence the extent of the auditor's fraud detection program, the principles enunciated here can be applied at departments of all sizes. Of course, outcomes such as loss prevention and recovering or saving dollars are always desirable.

PROCUREMENT FRAUD

Procurement fraud can occur during different phases of the procurement process by the initiation, delivery and payment for goods and services. The initiation process typically includes bidding and the creation of purchase orders; the delivery process includes the receiving and inventory functions; and the payment process encompasses the actual disbursement of funds. Computer assisted audit techniques (CAATs) applied to payment streams provide some of the most efficient means of testing both small and large amounts of data for detecting procurement fraud. By definition, data analysis and data mining techniques are highly dependent on underlying data, its existence, quality and integrity. Of the three phases of procurement noted above, the data-intensive payment function furnishes the best available data analysis prospects, and hence, that is the area we will emphasize in this article. Throughout this article we assume a fraud auditing team composition, whether or not part of the internal audit function, to include individuals equipped with a solid understanding of human behavior and possessing skills in accounting, computer programming, data bases, statistics, internal controls and business processes of the specific entity.[6]

THE FRAUD RISK HYPOTHESIS

Experienced auditors develop *fraud risk hypotheses*[7] when investigating one or more specific instances of fraudulent behavior: gathering, understanding and analyzing the available data, developing fraud risk hypotheses, refining them as necessary, arriving at two rival hypotheses eventually (for example, is this an unintentional error or is it deliberate fraud?; if fraud, what type of fraud scheme was employed?), and going about confirming one or the other.[8] In designing a fraud detection regimen, the government auditor uses a similar approach: The auditor must ask, "How could the system be exploited?" In other words, when performing a control systems vulnerability analysis the government auditor must scrutinize the potential weaknesses of the internal controls over the procurement process.

The government auditor should embrace both a controls orientation as well as a fraud risk orientation. A well-implemented system such as SAP, Oracle or PeopleSoft will include several built-in controls. Under the controls orientation approach, the auditor should look for possible breakdowns or circumventions of existing controls. Here, the auditor should not seek to duplicate tests already available, unless there is reason to believe that a controls breakdown has occurred. The auditor should also be aware of the extent to which the organization uses Electronic Data Interchange (EDI) to effect procurement transactions. The controls orientation contrasts with the fraud risk approach, which makes a rebuttable presumption about the "ineffectiveness of (existing) controls." Every critical aspect of the procurement process from the ground up is challenged, and the government auditor begins by: reviewing the procurement budget, identifying approval limits, purchase order initiation and processing, the use of credit cards and "smart cards," observing the general level of scrutiny over transactions, all the way through to ultimate authorized disbursement. Such a review must be supplemented by carefully designing tests to select transactions fitting each pattern and doing a "walk-through." In addition, it is important to recognize that the specificity of each test may increase with the size and complexity of the organization. For example, compiling a list of top vendors and contemplating the reasonableness of the list at a one-location, relatively small organization may prove effective, but attempting the same test without modification at a large, federal agency may not be as successful.

We now focus on the principles of fraud detection used to apply the fraud risk hypothesis approach.

Not all fraud schemes can effectively be detected using data-driven approaches. Instances of corruption—bribery, kickbacks and the like—and collusion consistently involve circumvention of controls. Searching relevant transaction data for patterns and unexplained relationships often fails to yield results because the information may not be recorded, *per se*, by the system. Behavioral concepts and qualitative factors frequently allow the auditor to look beyond the data, both with respect to data that is there and data that isn't.

Case Study

The following case demonstrates an effective application of a fraud risk hypothesis to an audit of procurement card transactions.

Analyzing the Data

Procurement credit card data provided in this case included all transaction information for all procurement cards for several years. The department properly controlled access to the cards, which meant the auditors could link all transaction data to the individual purchaser.

Developing Risk Hypotheses

The analysis focused on the transaction level and determined that fraud could surface in the form of unexplained patterns or significant cost overruns. Based on the controls over access, the auditors hypothesized a high risk of a perpetrator making purchases from a familiar vendor. Thus, the auditors designed tests to find large deviations from past history, wide disparity among seemingly similar cards, or a large number of purchases from the same vendor or group of vendors. These tests provided the highest potential for detection.

Confirming Risk Hypotheses

A summary of each card's activity for each billing period identified several instances of significantly higher activity than the average. Only one such card, however, showed a higher than average activity without a reasonable explanation. Going back to the transaction detail, the auditors found that fuel purchases—a common and authorized use—comprised the majority of the activity. After quickly arranging the data by date and obtaining relevant information from the company, the auditors surmised that this particular driver would have had to drive continuously more than 1,000 miles a day to justify the amount of fuel he purchased.

Solving the Problem

The subsequent investigation identified the entirety of the scheme: Whenever he had to fill up the vehicle, his friends and family would meet him at the pump, and he would fill up all the vehicles courtesy of the procurement department.

PRINCIPLES OF EFFECTIVE PROCUREMENT FRAUD INVESTIGATION AND DETECTION

Know Your Data

Performers, advertisers, salespeople and the like operate under a similar principle, "know your audience." The slogan for detecting fraud is "know your data." The GIGO Effect—Garbage In Garbage Out—is particularly relevant in data testing. The most sophisticated data analysis capabilities cannot cure underlying defects or impurities in the data itself. First of all, it is important to gain an understanding of how the data fields in the system work together. For instance, does the invoice date really mean invoice date and is not subject to alteration or manipulation? Does the payment date represent the date the payment was processed or the date the check was written, etc.? Keep in mind that data mining is not expected to "cleanse the data." That is, success of the data mining effort is heavily dependent on data quality and integrity. Second, the auditor, or audit team must ensure that the test will really answer the intended question. Frequently, auditors will run a specific CAAT because it's "one of the tests." Government organizations run on budgets, and all work must fit under the budget umbrella. Therefore, auditors should design and run tests to provide the best answers first.

Know the Purpose, Nature and Scope of Your Tests

In terms of measuring performance, what are we most concerned about and how will we measure success: by the number of possible frauds uncovered (fraud incidence) *or* by the dollar value of the detected frauds (fraud impact)? The former does not consider the magnitude of the possible fraudulent activity. The latter requires the auditor to prioritize the tests from most effective to least effective and allocate resources accordingly. Tests must be aligned to satisfy pre-established performance criteria. Auditors should guard against performing tests that consistently isolate only widely known inefficiencies or low-dollar fraudulent behavior—it saps other precious resources. Additionally, properly designed tests can

also help distinguish between isolated occurrences and pervasive/systemic problems—another way of looking at fraud impact.

Know Your Tools/ Methods: Work Smart

What constitutes the best answers? With an unlimited budget, auditors could perform numerous tests and investigate all anomalies. Because budgets constrain the use of both time and personnel, the successful fraud detection program must maximize the trade-off between cost and effectiveness as shown in *Figure 1*.

The figure illustrates how to categorize audit testing procedures to prioritize. Auditors should obviously avoid tests in quadrants I and III. Tests in the unshaded area of quadrant II, such as customized and focused data base procedures, are the most preferred as they yield maximally discriminating test results. Despite the higher cost, these tests are rather sophisticated and, therefore, can provide consistently more effective results. It should be noted, that tests like digital analysis (also called Benford's Law, see "Other Tests" below) falling in quadrant IV, while superficially appearing to offer an equal degree of effectiveness, really only succeed in identifying the so-called "low-hanging fruit" that may not adequately address the auditor's fraud risk hypotheses.

Know Your Software Platform and Sampling Potential

Successful testing for procurement fraud, especially at the transaction level, in large organizational settings requires analyzing millions of records. And, rather than sampling a representative number of records, we can test the entire population of transactions using census sampling. Realistically, practically and functionally, only an enterprise data base such as Microsoft's SQL Server, IBM's DB2, or similar system can provide the processing power needed for comprehensive testing procedures. Less technologically proficient team members can be trained to use an application such as ACL or IDEA to connect to the main data base, so that the more familiar program acts as a front-end.

After determining and finalizing a battery of fraud detection tests that make the most sense, automating the process will dramatically increase the effectiveness of the tests. One-time, or *ad hoc*, queries serve limited functionality on a going-forward basis. Instead, transform the query into a one-click process. Each of these tools permits customization through the use of saved processes using variables and user-entered parameters. The most powerful software and hardware cannot compensate for poor or nonexistent personnel training. Successful auditors, whether from financial or technical backgrounds, typically motivate themselves to learn the relevant skills.

Figure 1: Prioritizing Audit Tests

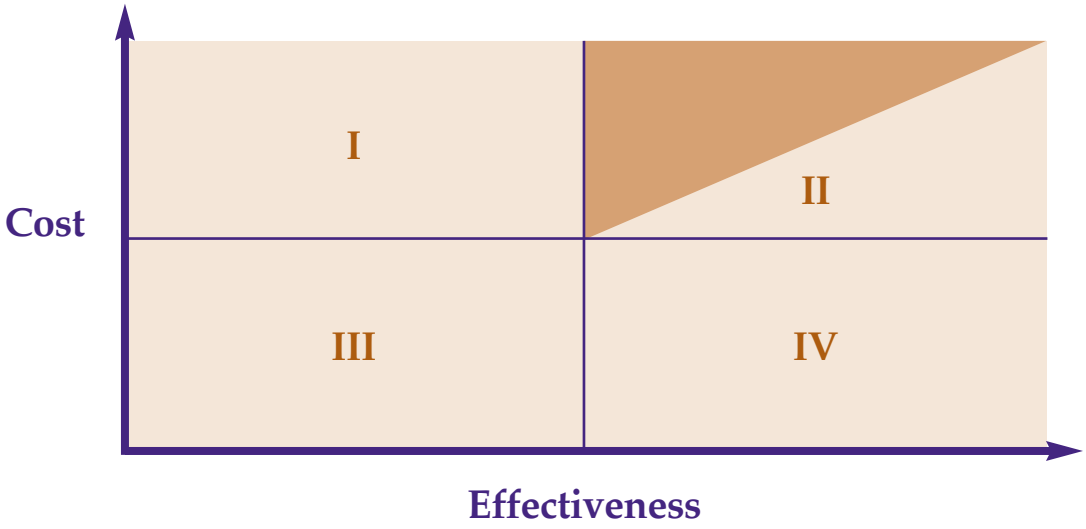


Figure 2: Decision Errors and Associated Costs

	Reality	
Decision	***Fraud is Not Present***	***Fraud is Present***
Fraud is Not Present	Correct Assessment	Type II Error *(Miss)*
Fraud is Present	Type I Error *(False Positive)*	Correct Assessment

Know the Signal-to-Noise Ratio

In testing procurement or other financial data for fraud (the signal), the risk for identifying false positives (noise) is present and increases dramatically with the size and complexity of the organization. To illustrate the signal-to-noise ratio principle and its ramifications for adopting a sensible fraud detection approach, we use the statistical concepts of Type I and Type II errors as shown in *Figure 2*.

A trade-off exists between controlling Type I and Type II errors such that decreasing one increases the other. Clearly, the goal must be to minimize Type II errors ("misses") by increasing the analytical test's power (or discrimination capability to distinguish a fraud pattern from other types of unusual variations in the data). Without any time, personnel or financial constraints, the auditor would design tests to reduce the risk of a Type II Error by accepting a larger number of *false positives*.[9] As budget and personnel constraints always exist, perhaps more so in a government agency, we should design tests to limit the number of false positives. Without advance planning, the auditor will likely experience a sort of "death by a thousand cuts" from an overwhelming number of red herrings, or red flags that are really only false positives. Limiting the false positives comes through two main areas. First, an inductive approach of identifying specific symptoms at an organization results in more targeted tests. Compare the following two tests as shown in *Figure 3*.

Figure 3: Designing Focused Tests

Original Test	Revised test
All purchase orders of more than $10,000 without proper approval	All cost centers (or other appropriate unit) with a quantity of unauthorized purchase orders of more than $10,000 greater than [some meaningful number]

Here the test has been customized to give the auditor more meaningful results by stratifying the population using cost centers and specifying additional criteria. Not only will this test reduce the number of false positives, but also it will be so much more useful in nonfraud applications. Such tests could also be randomized in terms of achieving total audit coverage over a pre-determined number of years.

The second method for reducing false positives involves changing the thresholds. If $10,000 gives too many hits, and $50,000 very few, try a number in the middle; or, if the concern is confined to a certain range, use that range. Essentially, the process uses trial-and-error to determine an optimum threshold level to use. However, the government auditor should also remain alert for so-called "tip-of-the-iceberg" occurrences that warrant a deeper investigation. For instance, the "trickle leading to the waterfall" hypothesis suggests that many frauds start out with small or immaterial amounts—sometimes because the perpetrator is testing whether the coast is clear—and over time cumulate to large, material amounts.[10]

After building the foundation of key fraud detection principles governing data analysis, we can focus on creating meaningful tests. The following section describes three main types of testing methods to apply in a fraud detection program.

DESIGNING THE TESTS

In this section, we consider the different types of testing that the government auditor might typically undertake: compliance testing, pattern analysis and other tests. What types of tests, when included as part of a fraud detection program, are likely to produce the best results? We now offer a discussion of each of the testing methods.

Compliance Testing

Compliance tests attempt to determine the extent to which the data complies with existing current laws and regulations, policies and procedures. Examples include testing for gaps in checks or purchase order (PO) numbers, proper approval for certain dollar thresholds, correct calculation of discount percentages, etc. Such tests typically belong as part of an effective internal control environment, but can quickly give the auditor helpful knowledge in designing other tests and understanding the state of the data. These more simple tests search for fraud risk factors and turn up Type I false-positives; however, in the context of process improvement, such false-positives may be true indicators of another nonfraudulent issue. After investigating the significant exceptions, each set of results can later be used as a cross-reference tool. Rather than spending time investigating each record extracted by the test, observe any consistencies across the tests. Does a particular location of the procurement department have a higher than expected instance of POs without approval, vendors with missed discounts, duplicate payments, etc.? On a limited budget, investigating each potential anomaly is impractical. Instead compare the results in a sort of cross validation, by determining what vendors, employees, etc. appear most frequently.

Pattern Analysis

Whereas the compliance tests described above compare data to certain expectations or procedures, this section describes testing for the unknown. Off the cuff, most auditors cannot estimate the average invoice amount for the top 25 vendors of their respective organization, or the average change in product price from period to period. Each organization has certain characteristics and trends that most transactions seem to follow. Does your agency purchase materials or services more at the beginning of a budget period than the end? How often do your suppliers change prices? The sheer volume of activity in a large organization masks the simplicity of improprieties such as false billing and improper payments schemes. In a sense, such schemes "slip through the cracks" of supposedly watchful eyes, only to be discovered by chance. This is why creating precise custom searches is so effective and important.

Other Tests

Tests in this category include those where additional training and resources result in more sophisticated analysis. Statistical analyses such as histograms of procurement transactions, multiple regression techniques, etc. can reveal unique trends and characteristics. Traditional tests and analyses such as vertical and horizontal analysis as well as fluctuation analysis may be less successful in revealing such trends. Data warehouse and data mining packages included in data base systems or purchased as separate applications can identify myriad characteristics, patterns and tendencies of the data. The advantage of using a data warehouse approach is that the auditor performs the analysis using an OLAP (Online Analytic Processing) data base, as opposed to an OLTP (Online Transaction Processing) data base. The design of the OLTP data base allows the quick and accurate recording of "operational data," but does not easily permit the type of analysis of "informational data" that an OLAP data base provides.[11] Additionally, these tests can incorporate many features of the previous tests for even more efficient processing and discovery of hidden relationships in the data. Neural networks, an artificial

intelligence technology that has powerful pattern recognition capabilities, act on data by detecting an existing, hidden, underlying organization.[12] These patterns can then be compared to information received on a real-time basis. However, these are fairly sophisticated data mining and fraud detection tools.

Digital analysis uses the principles of Benford's law and detects irregularities in the expected digital frequencies in a list of numbers. Essentially, Benford's Law explains the counter-intuitive phenomenon that numbers beginning in a one or two appear much more frequently—a combined 48 percent of the time—than numbers beginning with an eight or nine. Testing for adherence to this law requires a conforming data set and functional software. Without artificial influences, such as approval limits, a spike or decline in the expected frequencies denotes an anomaly. Further investigation will demonstrate the root cause of the variation, whether sourced in fraud or caused by unnatural distortions such as approval limits.[13]

CONCLUSION

Procurement fraud leads to the diversion of scarce resources for inappropriate, illegal, ineffective or inefficient purposes. Beyond preventing obvious abuse, the government has an obligation to modernize its priorities, practices and processes to cope with the demands and needs of today's changing world. This article presented the logic and rationale behind numerous data-driven analytic approaches that could be profitably used by the government auditor in detecting procurement fraud.

Effective fraud detection continues to move from simple, control-oriented Computer Assisted Audit Techniques (CAATs), to complex data manipulations and financial analyses. In the context of a procurement process, properly designed tests separate an effective program that generates tangible benefits from those likely to be forgotten at the next budget season. Such success occurs because auditors approach the detection process using principles, rather than canned, predictable checklists. Sound principles drive data-intensive audit testing strategies, which are likely to be relatively unpredictable, efficiently designed and rigorously implemented. Intuitive auditors can apply such proven detection principles to myriad situations using various tools with the intent of continually reducing the amount of money lost to procurement fraud in government. We are hopeful that the principles of data-driven fraud detection techniques will allow for enhanced auditing processes and equip government auditors in fighting procurement fraud, waste and abuse in their respective contexts. ■

Authors' Note

The views expressed in this article are the authors' personal views and should not be attributed to, nor be construed as reflecting the endorsement of, Ernst & Young LLP. We would like to thank James Grosskopf for his helpful comments on an earlier version of this article.

End Notes

1. GAO Report, *FEDERAL BUDGET: Opportunities for Oversight and Improved Use of Taxpayer Funds*, June 18, 2003, p. 8.
2. Indeed, "the determination as to whether a particular act is illegal would generally be based on the advice of an informed expert qualified to practice law or may have to await final determination by a court of law." (AU sec. 317, SAS No. 54: *Illegal Acts by Clients*, para .03, AICPA Professional Standards, New York).
3. GAO Report, *FEDERAL BUDGET: Opportunities for Oversight and Improved Use of Taxpayer Funds*, June 18, 2003, p. 20.
4. *2002 Report to the Nation on Occupational Fraud and Abuse*, Association of Certified Fraud Examiners
5. GAO Report, *FEDERAL BUDGET: Opportunities for Oversight and Improved Use of Taxpayer Funds*, June 18, 2003, p. 38.
6. Albrecht, Steven W., Albrecht, Conan C. "Root Out Financial Deception," *Journal of Accountancy*, April 2002.
7. Some practitioners refer to the use of fraud risk hypotheses as adopting the "fraud theory approach."
8. Wells, Joseph T. "Sherlock Holmes, CPA, Part 1," *Journal of Accountancy*, August 2003
9. Since Type II errors cannot be quantified since we cannot determine how many frauds we failed to detect (excepting in analyses containing historical data of "flagged" cases), we must increase the risk of Type I errors to control the Type II error rate; there is thus a Type I/Type II error trade-off.
10. In these cases, the fraud perpetrator adopts the technique of continuously "flying just below the radar" (below materiality thresholds or limits that may require authorization); nevertheless, over time, the cumulative amount embezzled or assets misappropriated usually constitute a material amount.
11. "Just What Are Cubes Anyway? (A Painless Introduction to OLAP Technology)," Published in the Microsoft MSDN library at *www.microsoft.com*, April 2002; Business Intelligence Certification, IBM Redbook SG24-5747-00.
12. Ramamoorti, S., and Traver, R., *Using Neural Networks for Risk Assessment in Internal Auditing: A Feasibility Study*, The Institute of Internal Auditors Research Foundation, 1998.
13. For the conceptual background behind Benford's Law and the necessary technical skills, auditors should read and become familiar with ACL's Benford's Law testing capability and Dr. Mark Nigrini's research behind it. See Nigrini, Mark J. (2000) *Digital Analysis Using Benford's Law: Tests and Statistics for Auditors*, Global Audit Publications.

Sridhar Ramamoorti, Ph.D., ACA, CPA, CFE, CIA, CFSA, CRP, a member of AGA's Chicago Chapter, is assistant director of Thought Leadership in the Global Investigations and Dispute Advisory practice of Ernst & Young LLP in Chicago, IL. His thought leadership activities include global practice development and product/service innovation, practice support, academic partnering and research/professional publications.

Scott Curtis, CPA, CFE, is a senior consultant in the Global Investigations and Dispute Advisory practice of Ernst & Young LLP in Chicago, IL. His professional experience is in the areas of fraud detection and investigation focusing on data analysis and in other technology-related areas. He has implemented fraud detection programs at* Fortune *500 companies and has developed training programs for professional accountants.