5-2013

Standard Costing Variances: Potential Red Flags of Fraud?

Cecily A. Raiborn
Texas State University

Janet B. Butler
Texas State University

Lucian Zelazny
University of Dayton, lzelazny1@udayton.edu

STANDARD COSTING VARIANCES: POTENTIAL RED FLAGS OF FRAUD?

Standard cost variances are commonly used to highlight operational strengths and problems, and their presence may be an indicator of fraud.

CECILY RAIBORN, JANET B. BUTLER, AND LUCIAN ZELAZNY

All organizations, regardless of size or activity, are vulnerable to fraud. However, manufacturing firms seem to be particularly vulnerable; a 2010 global survey of companies operating in more than 20 industries found that the manufacturing industry had 10.7 percent of all reported fraud cases, making it the second highest on the list.[1] Equally serious is the financial impact of these fraud cases. Manufacturers reported a median cost of $300,000 per reported incident, an amount nearly 90 percent higher than the median for all companies surveyed.

Despite the fact that organizations institute a wide variety of internal controls to deter and detect fraudulent activities, approximately 40 percent of fraud is initially detected through tips from stakeholders such as employees, customers, and vendors.[2] Unfortunately, the likelihood that a stakeholder will report fraud is reduced by factors such as personal job security concerns and/or whether management is involved in the fraudulent scheme.[3] Given that manufacturing has been significantly impacted by layoffs and economic downturns, internal tipsters may be less likely to come forward because of concerns about continued employment. Most manufacturers, though, have an important reporting tool that can help them detect fraud without the use of whistleblower tips: the standard cost variance. Standard cost variances are commonly used to highlight operational strengths and problems, but these reporting mechanisms can also

CECILY RAIBORN *is the McCoy Endowed Chair in Accounting at Texas State University – San Marcos. She received her Ph.D. from Louisiana State University. Her areas of teaching and research are financial and cost/managerial accounting, corporate social responsibility, and business ethics. Some of her articles have been published in the* Journal of Business Ethics, Journal of Corporate Accounting and Finance, Business Horizons, CPA Journal, *and* International Journal of Business Performance Management.

JANET B. BUTLER *is an associate professor of accounting at Texas State University – San Marcos. She received her Ph.D. from the University of Georgia, and teaches and researches in the areas of accounting information systems, environmental reporting, and cost/managerial accounting. Some of her articles have been published in* Issues in Accounting Education, Strategic Finance, Management Accounting Quarterly, the Journal of the American Taxation Association, *and* Advances in Management Accounting.

LUCIAN ZELAZNY *is an assistant professor of accounting at Texas State University – San Marcos. He received his Ph.D. from Virginia Tech. His areas of teaching and research are accounting information systems, cost accounting, IS audit, and cultural issues in systems development.*

serve as useful "red flag" indicators to help manufacturers identify fraud.

This article focuses on how standard cost variances can be used in detecting potential fraudulent activities. Each primary type of variance (material, labor, and overhead) is addressed with a discussion of possible inappropriate causal factors. Additionally, internal controls, graphic techniques, and other methods that can be implemented to combat fraud are provided.

Internal controls, standards, and variance analysis

An internal control (IC) is any organizational process used "to provide reasonable assurance regarding the achievement of objectives in the following categories:

- reliability of financial reporting;
- effectiveness and efficiency of operations; and
- compliance with applicable laws and regulations"[4]

The three basic classifications of ICs are preventive, detective, and corrective. A preventive control is focused on precluding either the occurrence of a specific error or irregularity or the nonoccurrence of a specific control objective. In contrast, a detective control identifies errors, irregularities, or unachieved control objectives after an undesired event occurs; the inappropriate actions may have either eluded, or were not the focus of, the preventive controls. In other words, detective controls draw attention to — but do not correct — a problem. A corrective control is designed to help a firm recover from undesirable or unauthorized activities.

Financial and operational planning requires estimates about future prices and usage of inputs. Standards specify expected costs and/or quantities for manufacturing a single unit of product or performing a single service. Managers commonly use standards to estimate future quantity requirements to help determine purchasing needs for material, staffing needs for labor, overhead capacity, and company cash flows. Standards also express the expected price to be paid for material, rate to be paid to labor personnel, and amount to be incurred relative to variable and fixed overhead.

An important benefit of standard costs is having norms against which actual operating activities can be compared, so that managers are able to assess operational effectiveness and efficiency. A well-designed variance analysis system will compute variances as early as possible so managers can monitor operations, detect deviations from the norm, ascertain variance causes, and take any necessary corrective actions. As with all business processes, the variance system is subject to cost–benefit constraints. Because undue investigations are expensive and inefficient,[5] supervisors often employ the management-by-exception principle to distinguish between situations that can be ignored and those that need attention. To implement management by exception, upper and lower tolerance limits of acceptable deviations from the standard are established. If a variance is outside of the tolerance limit, the variance should be investigated and its cause ascertained. Variance causality can be determined through observation, inspection, and inquiry. Management should then take action to eliminate unfavorable variances (or, on occasion, to continue favorable variances into the future).

Although managerial action is generally not required if variances are within an acceptable range, upper management should be aware of ongoing trends in variances. A consistent, albeit small, variance might indicate the beginning of a major problem. Additionally, variances are often interrelated and, therefore, cannot be analyzed in isolation from one another. For example, poor quality material may result in a favorable material price variance and an offsetting unfavorable labor efficiency variance. Minimizing total unit cost does not necessarily mean, given desired output quality standards, that the cost of each product or service input component should — or can — be minimized. Some possible input resource combinations are not necessarily practical or efficient. For instance, using low-tech equipment to minimize overhead depreciation charges may not be rea-

THIS ARTICLE FOCUSES ON HOW STANDARD COST VARIANCES CAN BE USED IN DETECTING POTENTIAL FRAUDULENT ACTIVITIES.

sonable in the manufacturing of high-tech products.

Variance analysis and internal control

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) [6] stated that an effective internal control structure has five components: the control environment, risk assessment, control activities, information and communication, and monitoring. Each component can be viewed with regard to a standard costing system or variance analysis.

Control environment. The control environment encompasses business actions, policies, managerial philosophies, and operating styles; it also creates an atmosphere within which internal controls exist. This atmosphere can enhance or hinder the effectiveness of ICs that have been developed for the organization. Implementation of a standard costing system indicates that management recognizes the importance of having benchmarks against which to measure actual outcomes. The level (expected, practical, or ideal) at which standards are set reflects the degree of commitment that management has to cost control, along with management's tolerance for deviations. When standards are set at the expected level, cost control is fairly lax and most outcomes will be within tolerance ranges. In contrast, ideal standards reflect exceptionally tight cost control but will potentially result in large unfavorable deviations.

IMPLEMENTATION OF A STANDARD COSTING SYSTEM INDICATES THAT MANAGEMENT RECOGNIZES THE IMPORTANCE OF HAVING BENCHMARKS AGAINST WHICH TO MEASURE ACTUAL OUTCOMES.

Risk assessment. Companies face many risks, and an effective IC structure will support assessment, analysis, and management of these risks. Neither a standard cost system nor variance analysis can help a firm predict future risks, but the standard setting process can force an examination of future market and labor conditions that may provide important information for the risk assessment process. Standard cost systems can also help in identifying the realization of some types of risk by highlighting when standards have not been met.

Control activities. Control activities are reflected in the policies and procedures used by a firm to ensure that management's wishes are accomplished. In general, a standard costing system's primary objective is cost control. As such, standard costing control activities include supervisory approvals or authorizations for purchases, materials issuances, labor rates, and contract commitments for fixed overhead costs. Consideration should be given to factors such as material quality, normal material-ordering quantities, expected employee wage rates, mix of employee skills, facility layout, and expected degree of plant automation. The entire variance analysis process is a control activity that supports operational and compliance objectives.

Information and communication. The control activities are facilitated by information and communication within an organization. The sharing of information helps when conducting and managing business operations, and it enhances the effectiveness of control activities. In the case of standard costs, information is communicated to appropriate parties throughout the organizational hierarchy so that all will know the basis on which performance evaluations will be made. Further, including various organizational areas (such as cost accounting, industrial engineering, human resources, and purchasing) when standards are developed helps to ensure their credibility. However, even with the most knowledgeable input, there will likely be variances between the standard and actual prices and quantities during any period. The materiality and assessment (favorable or unfavorable) of those variances will, as mentioned earlier, be linked to the level at which the standards are set.

Monitoring. Monitoring is an essential part of the IC framework and ensures that the control activities have been instituted, are functioning properly, and are up to date. In a standard cost system, monitoring occurs through the comparisons of actual and standard information made to ascertain operational effectiveness and efficiency. In addition, monitoring should be viewed as an ongoing process, and, relative to standards,

EXHIBIT 1 Summary of Variances as Fraud Indicators

Variance Name	Formula	Red Flag Indicator of Fraud
Material Price Variance (MPV)	(Actual Price – Budgeted Price) × Actual Quantity	*Unfavorable Variance* • Vendor kickbacks o Change to vendor with higher prices o Purchase of higher than specified material grade *Favorable Variance* • Vendor kickbacks o Larger than normal reorder quantities o Lower than specified material grade
Material Usage Variance (MUV)	(Actual Quantity – Budgeted Quantity Allowed for Actual Output) × Budgeted Price	*Unfavorable Variance* • Inventory Theft • Lower grade material was received than was ordered
Labor Rate Variance (LRV)	(Actual Rate – Budgeted Rate) × Actual Hours	*Unfavorable Variance* • "Out of the norm" labor rates for certain employees (real or ghost)
Labor Efficiency Variance (LEV)	(Actual Hours – Budgeted Quantity Allowed for Actual Output) × Budgeted Price	*Unfavorable Variance* • Employees overstating or "padding" hours worked • Presence of ghost employee
Variable Overhead (VOH) Spending Variance	(Actual Variable Overhead per unit – Budgeted Variable Overhead per unit) × Actual Quantity of cost allocation base	*Unfavorable Variance* • Theft of supplies • Fraudulent overtime *Favorable Variance* • VOH expenses inappropriately capitalized in non-inventory accounts
Fixed Overhead (FOH) Spending Variance	Actual Costs – Budgeted Costs	*Unfavorable Variance* • Ghost supervisory employee • Inflated payments made to related party (conflict of interest scheme) or to gain kickback *Favorable Variance* • Asset salvage value increased and depreciation reduced • Asset life extended beyond the norm and depreciation reduced • FOH expenditures inappropriately capitalized

Note: Standard prices, rates, quantities, or times may be inflated to game the system, leading to favorable variances.

it is reflected in the review and updating of standards to reflect changes in costs, quantities, and facilities.

The standard costing and variance analysis system is an IC tool that can help ensure operational efficacy and promote communication of expectations. In addition to these benefits, the system can be used to help management "identify areas of particular susceptibility [to

fraud] among employees in production, operations and administration."[7]

Variances as fraud symptoms

In the process of evaluating who or what was responsible for each variance, managers should be aware that variances (either unfavorable or favorable) can reflect both legitimate and illegitimate causal circumstances. Unfavorable variances occur when operations are less than the budgeted standards: Prices are higher or performance is lower than the standard. These variances cause operating income to decrease. Favorable variances reflect operations that are better than budgeted; as a result, operating income is increased. Both unfavorable and favorable variances for material, labor, and overhead may be red flag indicators of fraudulent activities (as presented in Exhibit 1). The following discussion focuses on recognizing the possibility that significant or ongoing standard cost variances could be symptomatic of organizational fraud.

MANAGERS SHOULD BE AWARE THAT VARIANCES (EITHER UNFAVORABLE OR FAVORABLE) CAN REFLECT BOTH LEGITIMATE AND ILLEGITIMATE CAUSAL CIRCUMSTANCES.

Unfavorable variances as indicators of fraud

Material. Because alternative material inputs can generally be used to generate similar output and output quality, the input choices that are made affect the price and quantity standards that are set. The choices result in trade-offs for material mix and yield, finished product quality, overall product cost, and product salability. The most common factor to explain a material price variance (MPV) is simply an increase or a decrease in unit cost; such a price change should be verifiable by investigating comparative market prices around the economic environment in which the purchases are being made.

Manufacturers need to be alert to the possibility of vendor kickbacks to purchasing agents and operations personnel when monitoring material prices and usage. A higher than expected price can result from payments to influence the vendor selection and/or the ordering process; a possible red flag indicator will be higher prices in conjunction with a vendor change. Another possibility that would create an unfavorable MPV is the purchase of a higher-grade material than that designated in the bill of materials. Although the primary cause (different grade material) might be identifiable, there is still a question as to the fundamental reason for such a purchase. Such purchases may be made because the designated grade of material may be unavailable. However, such purchases may also be made because of vendor kickbacks being made for purchasing the higher-grade material.

Large purchase orders, coupled with a significant unfavorable material usage (quantity) variance (MUV), could indicate inventory theft via collusion between the purchasing and receiving or delivery departments; materials delivery may be made to an unauthorized location for the benefit of the purchasing agent or another employee. Unfavorable MUVs may also arise without regard to material price variances. Such variances could result from inventory theft or from a vendor shipping a lower-grade material than ordered and continuing to charge the standard material price.

Labor. Labor rate standards should reflect employee wages and related employer costs for fringe benefits, FICA (Social Security), and unemployment taxes. In the simplest situation, all departmental personnel are paid the same wage rate as, for example, when wages are task specific or tied to a labor contract. If employees performing the same or similar tasks are paid different wage rates, a weighted average rate (total wage cost per hour divided by the number of workers) must be computed and used as the standard. Rate differences could be caused by length of employment or skill level.

The labor rate variance (LRV) is the difference between the actual wages paid to labor for the period and the standard cost of actual hours worked. Changing a payroll rate would generally require collusion between the hourly employee and someone in the payroll area. In large organizations, this circumstance would be unlikely due to the ability of large firms to segregate duties among many employees and to protect sensitive data files from unauthorized access; however,

it could occur in smaller organizations. In attempting to find fraud related to LRVs, an analysis should be run that highlights all "out of the norm" labor rates — which might be quite noticeable if union contracts are in effect. Trend analysis would indicate whether employees with higher rates are under the supervision of the same manager.

In contrast, the labor efficiency variance (LEV) indicates whether the amount of time worked was less or more than the standard quantity allowed for the actual output. Several potential fraudulent scenarios exist relative to unfavorable LEVs. Employees may be overstating or "padding" the number of hours worked. While there is a wide range of ways for employees to record their hours, there are two likely possibilities: Either the employee simply falsifies his/her timesheet and the supervisor is unaware of the discrepancy, or there is collusion with a supervisor to approve additional time.

An unfavorable LEV may also indicate the possibility of one or more ghost employees on the payroll. Ghost employees receive paychecks but provide no productivity; thus, labor efficiency would be below that which was expected. The perpetrator of a ghost employee scheme is likely to be either a supervisor who has not communicated an employee's departure or dismissal to the payroll department or a payroll employee who has not deleted a former employee from the system (or has simply "created" a ghost and placed him/her on the payroll). If the ghost is a former employee, the perpetrator is likely in collusion with that individual — unless the perpetrator has the ability to obtain and cash/deposit the ghost's paycheck.

Variable overhead. Variable overhead (VOH) covers a range of cost elements and fluctuates in a direct relationship with some designated level of activity (such as direct labor or machine hours). It is impossible to investigate for fraud using the total VOH spending or efficiency variance; variances in each cost element must be analyzed separately. VOH spending variances are caused by both component price and volume differences. VOH spending variances are often associated with price differences that have not been properly included in the standard rate; however, potential fraud causes of indirect material and indirect labor variances may also exist (and reflect scenarios similar to those of direct material and direct labor). Waste or shrinkage of production inputs (such as indirect material) is included in the VOH spending variance; such a category might be a prime location to hide supplies theft. In addition, an indirect labor variance that could be attributed to fraud is overtime — either relative to rates or hours — which may reflect collusion between an employee and payroll personnel or a supervisor; such a circumstance might be highlighted by running an exception report for employees who have received an excessive amount of overtime in a given period. Many of the other VOH cost categories reflect prices charged by external parties and, as such, would have limited potential for fraud.

The VOH efficiency variance quantifies the effect of using more or less of the activity or resource that is the base for VOH application. Thus, if VOH is applied on a direct labor hour basis, the VOH efficiency variance will track in tandem with a labor efficiency variance and is the result of the causal direct labor factors.

Fixed overhead. As with variable overhead, fixed overhead (FOH) is comprised of numerous cost elements including production and supervisory salaries, straight-line depreciation on factory assets, factory insurance, and the fixed portion of mixed factory costs (such as utilities and maintenance). The FOH spending variance represents the differences between budgeted and actual costs for the numerous FOH components, although it can also reflect resource mismanagement. As with VOH variances, individual spending variances should be calculated for each FOH component. An unfavorable spending variance for salaries could reflect ghost supervisory employees on the payroll.

AN UNFAVORABLE SPENDING VARIANCE FOR SALARIES COULD REFLECT GHOST SUPERVISORY EMPLOYEES ON THE PAYROLL.

Favorable variances as indicators of fraud

Favorable variances, because they increase income, are sometimes not investigated

as carefully as unfavorable variances because manufacturers are more concerned with eliminating process inefficiencies; however, some favorable variances may signal fraud. For example, a favorable MPV may arise if materials are being purchased in larger-than-normal reorder quantities as a result of a vendor kickback scheme. A favorable MPV would also be the result of buying a lower-than-specified grade of material. This situation might occur because of a lack in availability of the designated grade, but kickbacks could also be a factor. In this circumstance, it is useful to review the MPV in conjunction with the MUV. Commonly, using lower-grade materials results in an unfavorable MUV and possibly an unfavorable LEV due to the necessity for rework. Capitalizing variable or fixed overhead expenses in non-inventory accounts would reduce actual overhead cost and create favorable VOH or FOH spending variance. Maintenance costs have often been capitalized in fraud situations, such as Rent-Way Inc.[8] A significant decline in the depreciation expense during a period should be investigated to determine if asset salvage values have been increased, or if asset lives have been extended beyond the norm; such techniques were heavily used in the waste management fraud case.[9]

Today's emphasis on performance-based compensation can create a powerful incentive for managers to inflate standard prices/rates or quantities/times — either through gaining access to data files or by influencing the standard setting process so as to "game the system." Inflated standards can make actual performance appear more positive. Inappropriate influence could arise, for example, by including an excessively high waste factor in the material quantity standards or downtime/rework factor in the labor time standard while knowing that such misuse or delay is unlikely to occur. Additionally, if overhead standards are inflated, year-end results will generate an overapplied overhead balance that, when written off as a negative adjustment to cost of goods sold, can suddenly make income meet or exceed expected targets.

THE MOST EFFECTIVE DETERRENT TO OTHER TYPES OF FRAUD REQUIRES MINIMIZING THE OPPORTUNITY TO MANIPULATE WAGE RATES, STANDARDS, AND OVERHEAD.

Combating fraud: A combination of low-tech and high-tech approaches

Companies should employ a variety of high-tech and low-tech methods to combat fraud. "Tried and true" methods to prevent and detect material-related fraud include implementation of policies about vendor diversification, partnership alliances, and primary/sole sourcing relationships. Trends relative to purchases from a particular supplier should be analyzed, especially in conjunction with ongoing orders from a particular purchasing agent. The materials market should be monitored periodically to ascertain that prices being paid are competitive. Lastly, if material quantity variances are becoming more noticeable, the material flow from the vendor to the shop floor may need to be traced by using physical flow information, bar coding, or RFID tags to determine if "bad" output is related to poor quality material input from a particular vendor.

The most effective deterrent to other types of fraud requires minimizing the opportunity to manipulate wage rates, standards, and overhead. Reports should be generated that highlight period-to-period wage adjustments, especially those made outside of the normal raise timeframes (such as quarterly or annually). Such reports can also indicate employees whose hours worked are considered "excessive" as defined by the organization in relationship to a normal workweek, although this would possibly adjusted for seasonal variations or rush jobs. Standards files should be password protected, and access should be limited to employees with the authority to change standards. For both labor rate and time standards changes, the employee's supervisor should be alerted to note any variance patterns and ascertain the sources of those variations. Procedures to assess the possibility of ghost employees are well established and include the following:

- independent corroboration between human resource and payroll departments of current employees;
- review of payroll records for employees lacking Social Security numbers;

EXHIBIT 2 Data Mining for Fraud (Assumes Ongoing Variances)

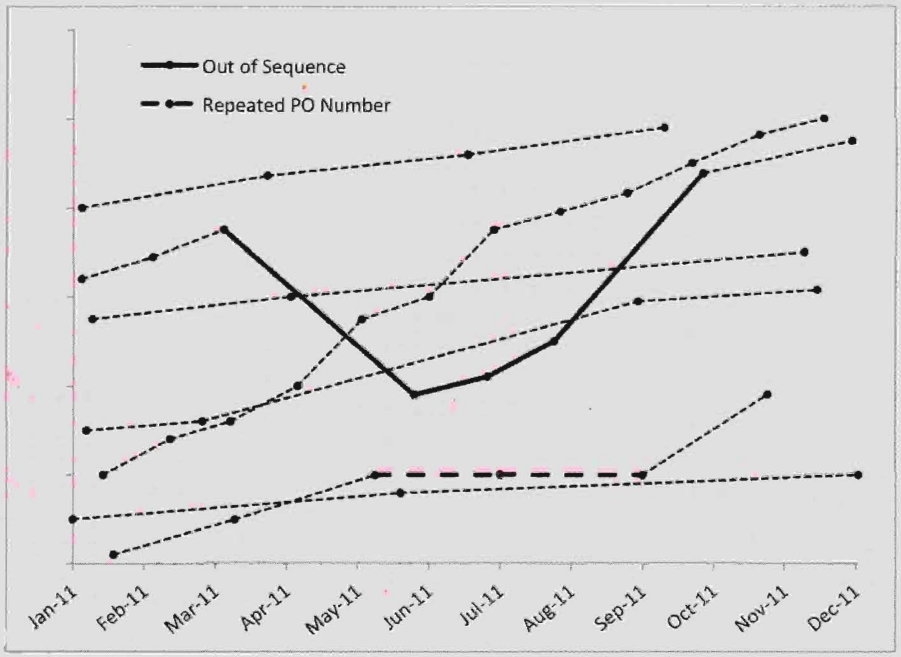
Variance(s)	Data Mined	Uncovers	Type of Fraud
Unfavorable material variance and favorable material usage variance	Accounts payable and material requisitions	Purchases made from same vendor	Kickbacks being paid to purchasing agent
Unfavorable or favorable material price variance	Accounts payable and employee records	Purchases made from same vendor; vendor has same address as purchasing agent	Shell company established by purchasing agent
Unfavorable or favorable material price variance	Accounts payable and employee records	Unnaturally consecutive invoice numbers	Shell company established by purchasing agent
Unfavorable material usage variance	Material requisitions, receiving reports, and employee records	Material requisitioned was delivered to alternate address	Employee theft of materials
Unfavorable labor rate variance	Personnel records and wages payable	Same supervisor for all overpaid employees	Collusion between supervisor and overpaid employees
Unfavorable labor efficiancy variance	Personnel records and employee timesheets	No timesheets for certain employees	Ghost employee
Unfavorable labor efficiancy variance	Employee timesheets and supervisor records	Falsified employee timesheets all all occurred under same supervisor	Collusion between supervisor and "absent" employees
Unfavorable variable overhead spending variance – indirect labor	Employee timesheets and overtime rates	Excessive overtime or excessive overtime rates paid to employees	Collusion between employee and payroll personnel or manager
Unfavorable fixed overhead spending variance – salaries	Personnel records and employee timesheets	A supervisor does not exist or is no longer with the company	Ghost supervisory employee
Unfavorable fixed overhead spending variance – depreciation	Asset aquisition records and depreciation calculations	Asset salvage value reduced or asset life extended beyong the norm	Management influencing performance-based compensation

- common deductions (such as insurance premiums or union dues);
- basic data (such as home address, phone number, or email);
- direct deposit information (although, depending on the organization and type of employees, lack of this information may be common); and
- cross-referencing duplicate employee information.

Variance analysis is helpful in drawing attention to certain types of fraud, but it can be somewhat limited in the information provided. To supplement the information gleaned through variance analysis, manufacturers should also leverage today's powerful and flexible technologies to detect fraudulent activities.

Data mining. Data mining is one example of a technology that can complement variance analysis in detecting fraud. Data

EXHIBIT 3 Visual Analytics of Purchase Order Numbers

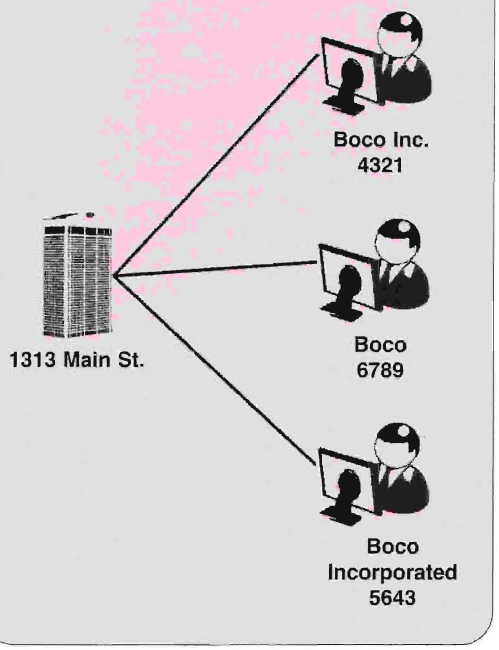


mining explores, aggregates, and analyzes large amounts of organizational data so as to "better understand business processes, trends, and opportunities [and] improve efficiency and effectiveness, as well as to discover anomalies."[10] Data mining is commonly used to discover significant patterns (especially those that might have been previously obscured) in the mined information — often to predict future behavior.[11] Therefore, after variance analysis highlights differences between actual and standard prices and quantities, data mining can be used to filter and sort individual transactions to identify similarities within the information (or to detect outliers that could be used to detect the possibility of fraudulent transactions). The data mining software is able to check relationships among multiple variables in multiple fields, so as to indicate implausible or surprising cases.[12]

For example, a data mining "drill down" may ascertain that a large portion of transactions causing a material price or usage variance share a common characteristic: All of them resulted from materials purchased from a single vendor. Additional comparative analysis might reveal that the vendor shares certain identifying information (e.g., phone number, fax, email, or address) with that of an employee — presenting a possibility of a pass-through or shell company. A shell company may also be a possibility if data mining shows that a vendor's invoice numbers are more consecutive than would naturally occur in a legitimate business. Another example of the use of data mining relates to a labor efficiency variance; data extraction may indicate that all labor inefficiencies occurred during a particular shift or under a particular shift supervisor. Additional scrutiny of the data logs might show a system override by the supervisor that allowed several "employees" to be added to the payroll records or inconsistencies and inaccuracies in personnel information. Exhibit 2 provides some examples of issues that might be uncovered after mining different types of information and the frauds that might be related to those discoveries.

Visual analytics. Visual analytics (VA) is another tool that can complement variance analysis in detecting fraud. VA uses a computer to create a representation of

EXHIBIT 4 Network Diagram of Vendors



complex data that is then subjected to human visual analysis — taking advantage of a human's ability to visually identify trends or patterns with which computers often struggle. This phenomenon is illustrated by the use of CAPTCHA technology to distinguish a human from a computer. CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It is typically implemented by warping the text, distorting the background, and adding lines, all in order to to make it difficult for automated routines to identify the text.

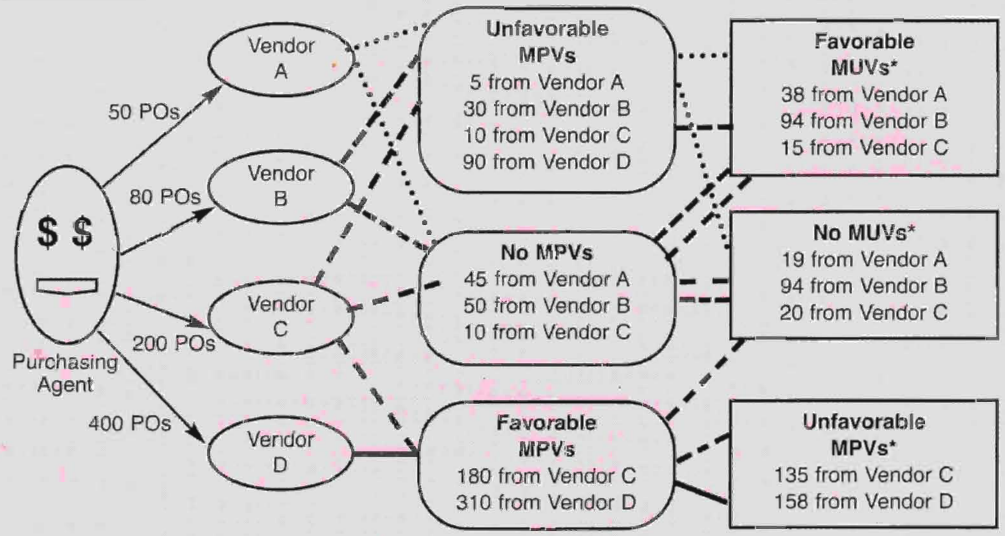
Thus, VA combines automated analysis processes with interactive visualizations to "enable detection of the expected and discovery of the unexpected within massive, dynamically changing information spaces," says Kris Cook, director of the National Visualization and Analytics Center. [13] Similar to data mining, VA can be used to identify connections and/or trends within the data that may be difficult to discover using traditional techniques. For example, as illustrated in Exhibit 3, VA may be used to generate an analysis of purchase orders for multiple vendors over several years. The chart highlights purchase orders from the same vendor by connecting them with a line, which can then be inspected for unexpected trends. Purchase order numbers that occur out of sequence or are repeated are easily identified and may indicate a fraudulent purchase order. With an online interactive chart, further investigation can take place by clicking on the purchase order to retrieve the details of that transaction.

Another example of visual analytics is a network diagram of vendors and addresses, such as the one shown in Exhibit 4. In this example, the approved vendor list has three vendors at the same address with similar names and different vendor IDs. While the most likely cause of this situation is that vendors were entered without thoroughly checking to see if the vendor information was already in the system, there is the potential for the duplicate vendors to be used in a kickback scheme, shell company, or other type of fraud. Invoices from (and payments made to) the duplicate vendors should be investigated.

Link analysis is another VA tool that allows relationships, especially those that are hidden in complex networks, to be seen in a "web" diagram. Exhibit 5 provides a link analysis among purchase orders, vendors, and standard cost variances. This diagram indicates that management may want to investigate why the purchasing agent is primarily buying materials from a vendor that, although selling at below market prices and generating favorable material price variances, provides inputs that appear to be of inappropriate quality due to the generation of unfavorable material quantity variances.

Today's enterprise systems integrate all functional areas of an organization to capture all aspects of transactions — with the data centrally located in one database rather than in disparate systems. The ability provided by data mining to easily "drill down" into transactional details helps mitigate risk by allowing the examination of an entire data population and the relationships between and among the data (rather than simply reviewing a limited data sample). [14] Additionally, the capa-

EXHIBIT 5 Link Analysis of Vendors and Variances



* All material is not issued in the same quantities or the same period as POs.

bility of visual analytics to expose data's "latent knowledge" without any hypotheses about variance causality also provides managers with a valuable tool.[15] Managers no longer have to rely solely on judgment to ascertain the meaning behind a variance computation; data patterns and relationships can be highlighted with data mining and VA techniques.

Conclusion

A manufacturer (or any other organization) that does not act on situations exposed by detective controls (such as variances) risks losing a substantial amount of money.[16] Early identification of fraud is particularly important because once the fraudulent actions have "infected" the accounting system, recognition of the problems becomes exceedingly more difficult. For example, if standards are inflated in the current period, those standards will likely serve as the basis for analysis until management orders a standard costing system review. Cost or rate increases may simply be "added on" to the fictitiously inflated standard — generating larger favorable variances and the potential for even greater bonuses. If ghost employees have been placed on the payroll, those "employees" will likely remain and continue receiving checks until a detailed human resource review is performed.

Ignoring standard cost variances or accepting superficial explanations for those variances dramatically minimizes the functionality of the detective internal control provided by variance analysis. Data mining and graphical techniques (such as visual analytics) can help explain standard cost variances, and they can enhance a manager's ability to identify problem areas and fraud. Technology augments human ingenuity by providing users with greater context and depth of information.[17] Not leveraging the tools available to investigate and recognize potential fraudulent causes of standard costing variances strengthens the opportunity to commit fraud.

Variances are often overlooked as fraud indicators. One reason that managers may not act on suspicious variances is that in analyzing standard cost variances, management commonly tends to accept the "easiest" or first explanation provided. In doing so, management is acting in conformity with a version of a 14th century line of reasoning referred to as Occam's razor (principle) or the

rule of simplicity. In its most minimalist form, this principle indicates that, while many possible explanations may exist for an outcome, the simplest reason is often the correct one.[18] However, such a "minimalist" version is not a complete one: Occam's razor actually continues further to state that additional circumstances should be examined to ascertain whether they provide more compelling arguments. Therefore, management must use all techniques at its disposal to delve into what might be underlying fraudulent causes for variances. Although definitely *not* the cause of all standard cost variances, fraud cannot be ruled out unless managers seek to discover the real causes rather than relying on Occam's razor's easy explanations. ■

NOTES

1 Association Of Certified Fraud Examiners (ACFE), *Report to the Nations on Occupational Fraud and Abuse*. Available at http://www.acfe.com/rttn.aspx (2010) (accessed Nov 26 2011).

2 *Ibid.*

3 Feldman, Y. and Lobel, O., Decentralized enforcement in organizations: An experimental approach, *Regulation & Governance* 2, no. 2 (2008): 165–192.

4 Public Company Accounting Oversight Board (PCAOB), *AU Section 319 Consideration of Internal Control in a Financial Statement Audit*. Available at http://pcaobus.org/Standards/Auditing/Pages/AU319.aspx (2002) (accessed May 13 2011).

5 Moffett, R. and Grant, G., Internal controls and fraud prevention, *Internal Auditing* 26, no. 2 (2011): 3–12.

6 Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control — Integrated Framework Executive Summary* (New York: AICPA, Sept 1992).

7 Martin, A., Data mining enables organizations to gather greater intelligence, *Internal Auditing* 24, no. 4 (2009): 18–22.

8 U.S. Securities and Exchange Commission (SEC), *Securities and Exchange Commission vs. Rent-Way, Inc., Jeffrey Conway, Matthew Marini, and Jeffrey Underwood*. Available at http://www.sec.gov/litigation/complaints/comp18241.htm (2003).

9 U.S. Securities and Exchange Commission (SEC), *Securities and Exchange Commission vs. Dean L. Buntrock, Phillip B. Rooney, James E. Koenig, Thomas C. Hau, Herbert A. Getz, and Bruce D. Tobecksen*. Available at http://www.sec.gov/litigation/complaints/complr17435.htm (2002).

10 Gelinas, U.J., Dull, R.B., and Wheeler, P.R., *Accounting Information Systems (9th ed.)*. (Ohio: South-Western Cengage Learning, 2011).

11 Chowdhury, S., A soft computing environment for data mining, *The Business Review-Cambridge* 18, no. 1 (2011):14–19.

12 Meidan, A., Data mining for forensic investigators, *Internal Auditing* 26, no. 1 (2011): 26–29.

13 Lemieux, V., Visual analytics: A new way to manage data deluge in e-discovery, *Information Management Journal* 45, no. 2 (2011): 38–40.

14 *Op. cit.* note 7.

15 Jans, M., Lybaert, N., and Vanhoof, K., A framework for internal fraud risk reduction at IT integrating business processes: The IFR2 framework, *International Journal of Digital Accounting Research* 9 (2009): 1–29.

16 Johnston, R. and Spencer, R., The right internal controls prevent fraud and loss, *Financial Executive* 27, no. 6 (2011): 60–63.

17 Conz, N., Finding patterns in the dark, *Insurance & Technology* 35, no. 1 (2009/2010): 32.

18 Fjelstad, J., Reversing the electronic assembly process, *Semiconductor International* 32, no. 13 (2009): 24–28.