iTK TECHNOLOGIES

BeyondPerformance

PROCURE TO PAY

Detecting & Preventing Accounts Payable Fraud, Waste & Abuse

When Sarbanes-Oxley was passed in 2002, many organizations were forced to take an in-depth look at internal Accounts Payable controls. Implementing internal controls takes time, but may prove to be a very cost-effective measure if any fraud or other leakages are found.

There are two ways to minimize the risk of fraud, waste and abuse in your accounts payable process:

- **Create preventative controls in your ERP to insure that roles support your segregation of duties objectives.**
- **Create controls and tests against your ERP system that detect when fraud, waste, and abuse is in process.**

This paper discusses both scenarios since when both are implemented and managed you are most likely to achieve your objectives.

Separation of duties (SoD) (also known as "Segregation of duties") is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and mistakes. A good Segregation of Duties control environment helps prevents fraud, waste, and abuse.

The accounting profession has invested significantly in separation of duties because of the understood risks accumulated over hundreds of years of accounting practice. Separation of duties is commonly used in large organizations so that no single person is in a position to, for example, create a vendor or pay a vendor without detection. Role based access control is frequently used in ERP systems where SoD is required. User access reviews are frequently conducted to insure people assigned roles do not create conflicts, as well as employee add, delete, and changes. For example, terminated employees need to be deleted on termination. The author has a subscription based application to automate this process.

PROCURE TO PAY 2

To successfully implement separation of duties in information systems a number of concerns need to be addressed:

- **The process used to ensure a person's authorization rights in the system is in line with his role in the organization.**
- **The authentication method used such as knowledge of a password, possession of an object (key, token) or a biometrical characteristic.**
- **Circumvention of rights in the system can occur through database administration access, user administration access, tools which provide back-door access or supplier installed user accounts. Specific controls such as a review of an activity log may be required to address this specific concern.**

A **mitigating control** is type of control used in auditing to discover and prevent mistakes that could lead to uncorrected and/or unrecorded misstatements that would generally be related to control deficiencies. For example, a corporate controller has the ability to approve GL transactions but changes/approves the wrong amount in conjunction with another employee. A mitigating control would be instrumental in finding and therefore, preventing such mistakes. If a key control fails and a mitigating control is in place, it may prevent the resulting potential financial statement error from becoming material. In this case, a finance review meeting is suggested to review transactions posted as part of the close process.

Compensating Controls are less desirable than the segregation of duties internal control because compensating controls generally occur after the transaction is complete (post audit.) Also, it takes more resources to investigate and correct errors and to recover losses than it does to prevent the errors in the first place. However, in some rare circumstances, organizational units do not have the staff resources to establish adequate segregation of duties. As a result of sickness a finance employee is authorized to create a vendor and pay a vendor for a few days. Compensating controls cannot be delegated because such delegation would defeat the purpose of the compensating control. The compensating control must be carried out by the Reviewer identified through the respective system access process. In addition, the compensating control review must be physically documented by the Reviewer.

PROCURE TO PAY 3

The **Management of Access Controls** for super administrative right of operating systems and applications is a substantial challenge for any IT controls environment. It prevents unauthorized access to key systems and databases because:

- **It keeps the group of administrators small and tightly managed (with secure log files to record activities where possible).**

It supports the activities with policy and procedural statements that prohibit administrators from reviewing files and folders with operational and business content.
In computer systems security, role-based access control (RBAC) is an approach to restricting system access to authorized users. It is used by the majority of enterprises with more than 500 employees, and can implement mandatory access control (MAC) or discretionary access control (DAC). RBAC is sometimes referred to as role-based security. Roles should not contain built-in conflicts. Additional issues and complexity occur when:

- **Users are assigned multiple roles**
- **User assigned rights by user ID**
- **User accessing multiple systems**
- **Users change roles or add roles(piggy backing)**

Let's spend the remainder of this paper reviewing the controls and transaction testing associated with capturing potentially fraudulent transactions before or after they have been posted. While manual testing and recovery services can capture some financial leakage they tend to be labor intensive and mistake prone. The best and most cost effective approach is to use AI based techniques that incorporate the analytics highlighted below to capture the following transactions before they have been posted. The author is one of the leading providers of a subscription based AI offering that addresses this Procure-to-Pay fraud, waste and abuse issue.

ITK TECHNOLOGIES

Beyond Performance

PROCURE TO PAY 4

1. Duplicate Payments

Duplicate payments in most cases may not be fraud-related, but continue to be a significant A/P leakage that is both preventable and recoverable. Mark Van Holsbeck, Director of Enterprise Network Security for Avery-Dennison, estimates that corporations make duplicate payments at the rate of 2%. Two percent may not sound like much, but if your company's A/P invoices total $75 million, duplicate payments may account for $1.5 million. Take a look at the statistics:

- **Medicare - The Dept of Health & Human Services' Inspector General estimated that Medicare made $89 million of duplicate payments in 1998.**
- **Cingular - We have once again discovered that payments made online as an Electronic funds payment for TDMA accounts, have been deducted twice from the customer's checking account.**
- **Medicaid - We identified at least $9.7 million in such duplicate payments during our two-year audit period, and estimated that as much as $31.1 million in additional duplicate payments may have been made."**

Many software packages have some controls over duplicate invoices but it usually takes in-depth querying to find them all. For example, many accounting packages do a duplicate invoice check and prevent you from keying in a duplicate invoice number for the same vendor. But just add an "A" to the invoice number or change a penny and you are on your way to a duplicate payment. Another common mistake is found in vendor files; duplicate vendor numbers for the same vendor is the number one cause of duplicate payments.

Here is what we recommend for developing an accurate and comprehensive dupe payment report:

I. Implement the 5 basic dupe searches if you haven't already. These are:

Report	Vendor #	Invoice #	Invoice Date	Invoice Amount
EEEE	Exact	Exact	Exact	Exact
EEED	Exact	Exact	Exact	Different
EEDE	Exact	Exact	Different	Exact
EDEE	Exact	Different	Exact	Exact
DEEE	Different	Exact	Exact	Exact

A programmer in your IT department will be able to help you with the SQL code for these joins. The SQL code will look something like this to create the first report “EEEE”:

```
CREATE TABLE DUPES_EEEE AS
SELECT A.*
FROM   INVOICES A, INVOICES B
WHERE  A.VENDORID=B.VENDORID AND
          A.INVOICENUM=B.INVOICENUM AND
          A.INVOICEDATE=B.INVOICEDATE AND
          A.INVOICEAMT=B.INVOICEAMT AND
          A.ID <> B.ID
```

The ID field should be a unique record identifier to distinguish one record from another. In Microsoft Access, these fields are usually created by using the data type “AutoNumber”. In open code, a field such as this can be easily created using a counter and incrementing it by 1 for every record (COUNTER = COUNTER + 1).

II. Implement some fuzzy-matching

Implementing “similar” fuzzy-matching instead of exact matching is what makes this approach more accurate and powerful than many. We define “similar” to mean the following:

Invoice numbers are considered similar if they are exact after stripping out any zeros and any alphabetic characters as well as punctuation characters.

Invoice dates are considered similar if the difference between the dates is less than a designated amount such as 7 days. For example, if you entered "7" days for the date tolerance, then all invoices with a date different of 7 or less would be considered similar. We generally set the date tolerance to 21 days to catch duplicate payments made 3 weeks apart; this often eliminates catching legitimate rent payments.

Amounts are considered similar if they meet one of three criteria:

1. the amounts are 5% +/- the other amount
2. one amount is exactly twice as much as the other, i.e. $220.15 and $440.30
3. the amounts start with the same first 4 digits, i.e. $123.45 and $1,234.55

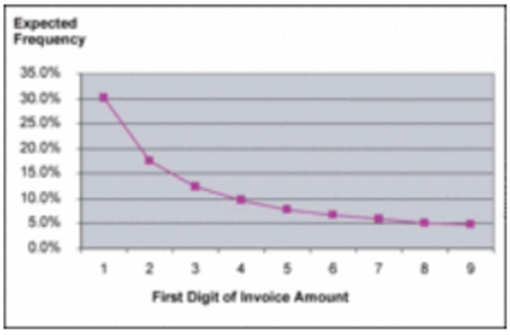
Try using similar matching on the invoice number, date, and amount fields when you conduct your next duplicate payment audit – your reports will be shorter and more accurate!

2. Benford's Law - What Is It?

Benford's Law (which was first mentioned in 1881 by the astronomer Simon Newcomb) states that if we randomly select a number from a table of physical constants or statistical data, the probability that the first digit will be a "1" is about 0.301, rather than 0.1 as we might expect if all digits were equally likely. In general, the "law" says that the probability of the first digit being a "d" is

Where ln refers to the natural log (base e). This numerical phenomenon was published by Newcomb in a paper entitled "Note on the Frequency of Use of the Different Digits in Natural Numbers", which appeared in The American Journal of Mathematics (1881) 4, 39-40. It was re-discovered by Benford in 1938, and he published an article called "The Law of Anomalous Numbers" in Proc. Amer. Phil. Soc 78, pp 551-72. [1]
You can actually re-create this function in Excel quite easily. In one column, type 1, 2, 3, through 9, making 9 rows in cells A1 through A9. In the second column, cell B1, type the function "=ln(1 + 1/A1) / ln(10)" and copy this function for cells B2 through B9 and it will create the probabilities.

How is it used to identify fraud?
If we know the normal frequency of digits, then we can identify digit frequencies that violate that normal behavior. For example, Benford concluded that, out of a group of numbers, the first digit will be "1" about 30% of the time. Similarly, using the same function, we can expect the first digit to be "8" about 5.1% of the time. Expected frequencies for each first-digit of the invoice amount are shown in the graph below:



PROCURE TO PAY

3. Rounded-Amount Invoices

People who commit fraud often create invoices with rounded amounts, which are invoices without pennies. Yes, you would think the fraudster would have "cents" enough to do otherwise. An easy way to identify rounded-amount invoices is to use the MOD function in Excel. Suppose your invoice amount is $150.17; then MOD(150.17,1) gives you the remainder of dividing 150.17 by 1, which is .17. So, using the MOD function with a divisor of 1 on a no-pennies amount would leave us a remainder of 0. Additionally, try to rank your vendors by those with a high percentage of rounded-amount invoices. To do this, just calculate each vendors' number of rounded-amount invoices and divide it by the total number of invoices for that vendor, obtaining the percentage. Then rank by descending percentage to review the most suspicious vendors first.

4. Invoices Just Below Approval Amounts

People who commit fraud are not always the "sharpest tool in the shed." Suppose an A/P clerk knows the different dollar thresholds for management approval. For example, a supervisor may only be allowed to approve invoices of $3,000 or less, while a manager may be allowed to approve invoices of $10,000 or less, and so on. Suppose this A/P clerk and a manager decide to skim off some extra dollars together. What is the easiest way to get the most money? Create an invoice just below the approval level of that manager: $9,998 when the approval level is $10,000; or $2,978 when the approval level is $3,000.

To identify these potentially fraudulent invoices, try this: identify invoices that are 3% (or less) LESS THAN the approval amount. For example, if your approval amount is $3,000, then any invoice that is between $2,910 and $2,999 would be flagged as suspicious.

5. Check Theft Search

Most Accounts Payable departments conduct a reconciliation of Accounts Payable with the monthly Bank Statement to identify any discrepancies between the two. This process can also be instrumental in identifying check fraud. One simple way to spot potential check fraud is to identify missing check numbers or gaps in reconciled checks numbers. This is usually indicated on the bank statement with a '*" or '#' to indicate the check number is not sequential.

Another more advanced way is to conduct a reverse Positive Pay electronically. By merging your check register, A/P file, and bank statements together, you have the power to identify stolen checks. Better yet, if your bank has OCR (Optical Character Recognition) abilities, then you can identify the actual payee on the check.

Speaking in technological terms, you have 3 different data bases describing 1 activity. Use the 3 data sources to find any discrepancies in the 1 payment. If your check numbers are unique, try merging all 3 data sources by the check number and compare each of the following fields:

-payee
-check amount
-check date

Using SQL code or another programming language, identify all of the checks that are in one data base and not the other. In addition, identify all of the checks that are in all 3 data sources but have different payee names or different amounts and dates.

6. Abnormal Invoice Volume Activity

Monitoring vendor invoice volume is one way to alert you to abnormal behavior. Rapid invoice volume increases may indicate a legitimate increase in business, but also may indicate that a fraudster has become more confident in stealing money. Either way, the increase may warrant further investigation. Suppose a vendor has 2 invoices one month and 70 the next – you may want to know why even if the reason is not a fraudulent one. To calculate the percent increase in invoice volume from month to next month, find the difference in number of invoices and then divide by the number of invoices in the first month. In our example, going from 2 invoices to 70, the difference (68) divided by the number of invoices in the first month (2) represents a 3,400% increase. Setting the threshold percentage is the key here; when doing audits, we like to set the threshold percentage at 300% or higher. Setting the threshold at 300% will catch increases from 3 to 13, which may not be interesting, so you may also want to set a minimum number of records that you are interested in, such as 50 as your second month's number of invoices. Setting the threshold at 300% will also catch more interesting increases, such as 50 to 220.

7. Vendors with Cancelled or Returned Checks

Cancelled and returned checks do occur in the course of a normal Accounts Payable month. What is more uncommon is a vendor with many cancelled checks or a regular pattern of cancelled checks. Cancelled checks are usually legitimate transactions; however, a cancelled check can be returned to the wrong hands and re-written to the fraudster. Below is a true story of how a clerk turned a returned check into a fraudulent one:

"An uncashed disbursement check was returned to an accounts payable clerk for disposition because she originated the invoice entry. The clerk put the check in her desk and forgot about it for several months. Upon cleaning her desk, she discovered the returned check. When she checked the paid history, she realized the supplier had returned the check when it was determined to be a duplicate payment of an invoice. She also noticed that the payee name had been printed slightly below "Payee" on the check. With a bit of effort she managed to align the check and insert her name above the original payee in a print similar to the original, along with an "or" designation following

her name. The fraud was caught by an accounts payable auditor searching for duplicate payments and who was asked by the supplier to furnish proof of duplicate payments by providing copies of both cancelled checks. “

This algorithm is easy to implement. Calculate the number of cancelled or returned checks for each vendor and divide by the total number of checks for that vendor. Then, sort this list by descending percent so that your most suspicious vendors are at the top of the report

8. Above Average Payments per Vendor

This algorithm identifies invoices that are way above average for a particular vendor. Suppose a vendor normally has invoices ranging from $1,000 to $3,000; suddenly an invoice shows up for $25,000. You may want to investigate this abnormality and can do so using this alert pattern.

This algorithm is also easy to implement: For each vendor, calculate the average and standard deviation of the invoice amount. Then, calculate a z-score for each invoice amount:

z-score = (invoice amount – average amount) / standard deviation

Then, flag all vendors with a z-score above 2.5, indicating the payment is more than 2.5 standard deviations above the mean. If your report is still too large, try increasing the z-score threshold to 3.0 or higher.

Using this algorithm alone, we were able to catch employee fraud occurring in a mid-size health manufacturing company. The fraudulent employee was receiving a paycheck every other week in the amount of $500 to $1,000 when, all of the sudden, 3 invoices for $40,000 each appeared. Because $40,000 was significantly greater than this employee’s average payment, the payments were flagged for further research. What made the invoices even more suspect was that they occurred on or near the same date and had no invoice number. After alerting the new controller of the suspect payments, the new controller was aware that an employee had left in a legal “scuffle” but was not aware of the $40,000 checks that were stolen.

PROCURE TO PAY

9. Vendor / Employee Cross-Check

"Trust but verify". Most employees are generally trustworthy! But it does not hurt to conduct some data tmining to make sure they are. Here is a simple approach to cross-check your vendor and employee files to see if perhaps an employee has set up a fictitious vendor.

Try merging your vendor file and employee file by the following variables:

- Address
- Tax ID Number
- Phone Number
- Bank Routing Number

If you have a good programmer, try doing some fuzzy-matching on these fields as well. For address, try extracting JUST THE NUMBERS in the street plus the zip code, and then compare these numbers. This eliminates matching on noise words such as "Drive" and "Suite".

Also, try doing some fuzzy-matching on tax ID number as well, just in case there was a typo in the data entry. If you specify that the tax IDs are equal if they are even 1 digit off, you may catch a vendor/employee ring!

This algorithm made it possible to detect a real employee ("Kathy") whose SSN was the same as a company EIN (tax ID number). The company name, which we will call "ABC Inc", happened to be on the same street, city, and state as a person with the same last name as the employee (presumably her spouse). Without this pattern, the employee fraud may have gone undetected.

10. Vendors with a Mail Drop as an Address

This algorithm compares vendor addresses with mail-box drop address such as "Mail Boxes, Etc". Some fraudsters will use mail drops as their address instead of a P.O. Box, to hide their fraudulent activity. Not all of the vendors appearing on this list will be fraudulent, because a vendor may in fact be right next to a Mail Boxes, Etc. However, the list provides a unique approach to reviewing vendors who also may show up on another alert list.

(To obtain a copy of the mail-drop table, contact the author of this document). Or, if you have time, you can also search for Mail Boxes, Etc. on www.411.com and put the addresses in a database and then conduct your address matching accordingly.

iTK TECHNOLOGIES

BeyondPerformance

PROCURE TO PAY

Summary

Occupational fraud, waste and abuse is a growing problem. In fact, the Association of Certified Fraud Examiners (ACFE) estimates that 5% of all revenue is lost to occupational fraud, waste and abuse every year. While fraud is not 100%preventable but there ARE steps you can take to both prevent and detect fraud, waste and abuse on an ongoing basis.

About the Author

ITK Technologies has created a unique AI based subscription service to streamline the SOD review process and uniquely enables the detection of financial transactions that create financial leakage. For example, duplicate invoice payments that may or not be intentional. This service can detect potential payments before, and/or after payment is made. This subscription service is available as a standalone option independent of the company's managed services program.

infor Gold Channel Partner