Article can be accessed online at http://www.publishingindia.com

SAP System as Vendor Fraud Detector

T. N. Varma*, D. A. Khan**

**Department of Computer Applications, NIT, Jamshedpur, Jharkhand, India.*
Email: tpverm@yahoo.com

***Department of Computer Applications, NIT, Jamshedpur, Jharkhand, India.*
Email: dakhan.ca@nitjsr.ac.in

Abstract

In the last decade, Enterprise Resource Planning (ERP) systems are one of the most important IT developments, which improve productivity and profitability of the organisation. SAP is the leading market player in ERP systems. The vendor master file in SAP is used to store information about critical and sensitive data of vendors and this data is target of fraudsters. However, fraud is increasing and it becomes a risk to supply chain management. Hence, it is a requirement to plug the opportunity of fraudsters by help of system. The present paper presents a review of red flags of vendor master, different vendor fraud etc. Further, this study makes the development of a prototype model for detection of vendor fraud based on analysis of SAP security log data, segregations of duties and fraudulent scenarios.

Keywords: ERP, Fraud, SAP, Vendor

Introduction

Organisations never suspect their employees because of their trust, reputation, or employee's length of service. When employees violate the trust, it leads to fraud. On other hand, organisations are dependent on vendors, an integrated part of Supply Chain Management (SCM), who provide materials or services to a company or individuals. An Enterprises Resource Planning (ERP) system is a software solution that aims to automate and integrate the core business processes of an organisation. Whilst, ERP systems provide numerous benefits to organisations, due to their complexity, they are vulnerable to many internal and external threats (Little & Best, 2003). SAP is an ERP system with high level of integration by utilising a single data model, developing a common understanding of what the shared data represents and establishing a set of rules for accessing data. The vendor master is a critical part of ERP system, in which vendor's related sensitive data as personal details of vendors, bank details, quotation details, payments, etc., are stored and vendors have access to sensitive information of organisations, which are creating risks to the organisation. ERP systems play a vital role in an organisation of generating the fraud in their supply chains, because vendor master being the target of fraudsters. Vendor fraud involves fraud schemes in which the fraudster manipulates vendor's sensitive data or a company's accounts payable and payment systems individually or in collusion with the organisational employees for illegal personal gain. Internal audit, being a primary tool detects and prevents fraud, but opportunities to commit fraud are exponentially growing. The traditional or manual audit approach is limited, because it reviews only a small percentage of a large population of transactions, which is difficult to analyse or monitor manually. Proactive fraud detection uses technology to rapidly analyse large sets of transaction data (Debreceny, Gray, Jun-Jin Ng, Siow-Ping Lee, & Yau, 2005), using IT to proactively detect fraud enables organisations to monitor and analyse large transaction datasets in real or near real time (Alles, Brennan, Kogan, & Vasarhelyi, 2006, Broady & Roland, 2008). The data related to vendors are stored in SAP tables (LFA1, LFB1, LFM1, LFBK, etc.) and all transactions are logged in different tables. Employees having SAP system authority can work as per their t-code authorisation. Hence, segregation of duties is essential against each user ID. The objective of this study is to detect proactively vendor frauds in SAP environment by using simply excel sheet with the help of user authorisation, system audit log of user activities and

abnormal change/modification in critical/sensitive data in vendor master.

Literature Review

Why people commit fraud was first examined by Donald Cressey, a criminologist, in 1950 with help of "Fraud Triangle". Donald R. Cressy studied the circumstances that led employees to be so overcome by temptation that they were driven to violate their position of trust (Wells, 2008, 2011). The three key elements of the fraud triangle are pressure (usually an un-shareable need), rationalisation (of personal ethics), and opportunity (knowledge to commit the fraud). Opportunity and its characteristics are present in an enterprise system. We can detect fraud proactively by continuous monitoring organisation's data. Continuous monitoring increases the probability of detecting fraudulent activities (Coderre & Warner, 1999; Potla, 2003). Huge data transactions are difficult to analyse manually in real-time. The alternative is to automate this process by using information technology (Broady & Roland, 2008). Many organisations consider the use of information technology (IT) to detect fraud. Automated fraud detection significantly reduces the labourious manual aspects of screening and checking processes and transactions in order to control fraud (Phua, et al., 2010). An anomaly detection is a process that creates fraud scenarios and identifies a means to detect each scenario (Islam, Corney, Mohay, Clark, Bracher, Raub, & Flegel, 2010), which may be useful in vendor fraud detection and prevention. Most occupational fraudsters exhibit certain behavioural traits as red flags that having unusually close associations with vendors or customers (22%) (ACFE, 2014). The Vendor Master file in an ERP system is an essential element of the procurement to pay cycle. In SAP, this contains vendor code, name, address, partner function, bank details, tax code, purchasing function etc. Several researchers discussed about the vendor fraud schemes. An employee may create a fake vendor in the system and submit false invoices for payment. The enterprise system may pay these invoices electronically directly into an employee's bank account (Best, Rikhardson & Toleman, 2009). Segregating vendor maintenance, invoice entry and payment can significantly reduce the risk of accounts payable frauds (Little & Best, 2003). Poor, incomplete or a lack of segregation of duties can, however, often provide opportunities for fraud schemes (ACFE, 2014). Early detection of fraud can limit losses and prevent the recurrence of such activities by proactively using information technology. A common type of fraud in the purchasing cycle involves fraudulent disbursements by collusion between an employee and the vendor. Fraudster may create a shell company and submit the fictitious invoices to an organisation for payment (Wells, 2002; O'Gara, 2004). An employee may create a fake vendor in the system and submit false invoices for payment. The enterprise system may pay these invoices electronically directly into an employee's bank account (Best *et al*., 2009). Vendor fraud occurs by access of fraudster to the ERP system of creation or modification of vendor master records and invoice entry sub-system (Narayan, 2008; Padhi, 2010). Data analysis techniques can be used to detect fraudulent activities that have already occurred as well as to proactively determine the propensity for frauds occurring in the future (Edge & Falcone Sampaio, 2009). Vendor master records can be created or modified in the following ways; a) create a fake vendor; b) temporarily modify an existing vendor (flipping); c) permanently modify an existing vendor; or d) use a one-time account (Singleton, Singleton, Bologna, & Lindquist, 2008). Invoices can be entered in an enterprise system for fake payment to the vendors in the following ways; a) by creating a fake invoice; ii) using a legitimate invoice; or iii) creating or using a duplicate invoice (Best, 2005). Existing fraud detection method typically analyse system log related to vendor and user activity logs in order to detect vendor fraud. Segregating vendor maintenance, invoice entry and payment can significantly reduce the risk of such frauds in the absence of collusion among personnel (Srinidhi, 1994; Little & Best, 2003). An application of continuous monitoring and the use of contextual meta-data to perform rich audit analyses. Several anomalies reported by the CM system were not detected by the organisation's internal auditors when they conducted their examination of the same data using conventional procedures. Such a system may potentially bring greater insights and transparency for continuous monitoring, assurance and organisational performance (Singh & Best, 2015).

Organisation of Paper

This study is based on essential steps of detecting fraudulent activities to answer the key research question: can SAP system be useful for proactive detection of vendor fraud? The following steps were adopted for this:

(a) understanding the business or operations - Introduction and Literature review, discussed in first two sections;

(b) cataloguing the symptoms that the most likely vendor frauds would generate - (i) design of con-

ceptual vendor fraud model in fourth section, (ii) vendor red flags in fourth section, and (iii) risks and perpetration of vendor fraud discussed in fifth section;

(c) creation of vendor fraud scenario for fraud detection: transformation of fraud symptoms into using SAP logs related to vendor fraud and invoice payment in seventh section;

(d) methodology used for vendor fraud detection and data analysis including data acquisition from SAP is explained in eighth section; and

(e) finding of result investigating suspicious transactions in ninth section.

This study is based on analysis of transaction data and audit logs captured from SAP system of an organisation. Since data is proprietary of an organisation, hence we had changed the actual figures.

Conceptual Vendor Fraud Model

There are three key elements - pressure, attitude (rationalisation), and opportunity (knowledge to commit the fraud) as per theory of Fraud triangle. In SAP system, fraudsters get opportunity due to system weakness, which is basis of development of this model. On that basis, weakness in vendor master was categorised as high and low and correlated with red flags. Then risks of fraud were divided into known vendor fraud and fraud due to collision of employee and vendor. These characteristics can be used proactively to detect fraud by analysis of SAP data and red flags.

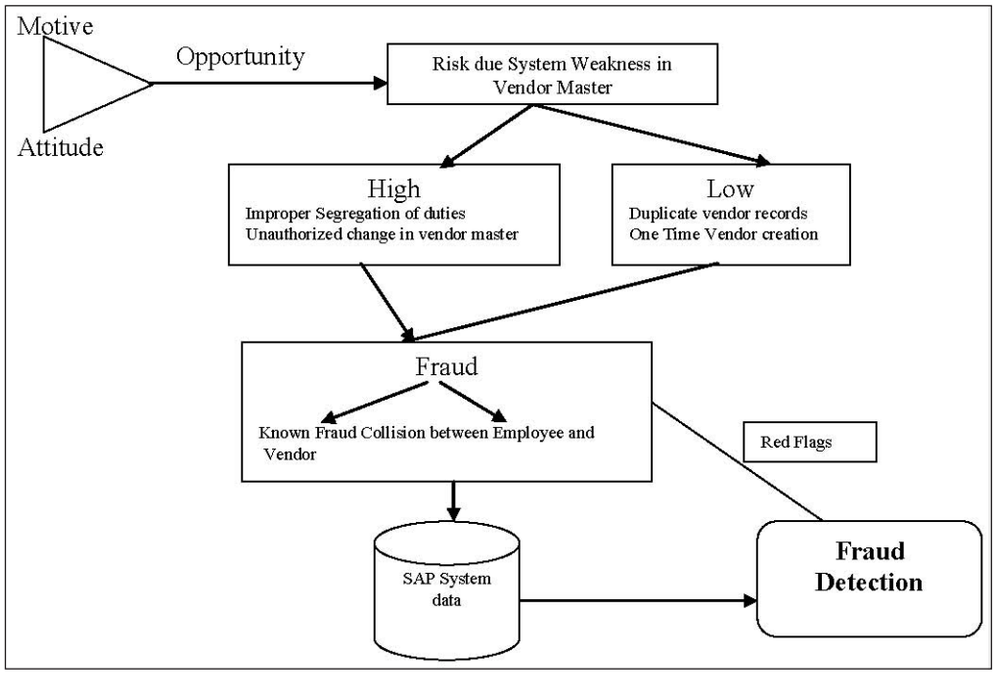

Fig. 1: Vendor Fraud Detection: Methodology

To develop this model, an element, opportunity of fraud triangle was only considered that motivates an individual to perpetrate fraud. Secondly, the model focuses on detection of vendor fraud in an organisation. This is achieved by: (a) creation of list of known vendor and fraud symptoms (red flags), (b) identification of risk due to system weakness in vendor master, (c) transformation of fraud symptoms into vendor fraud scenario with help of SAP t-code related to vendor master and vendor payment, (d) experiments with SAP system log data related vendor master, and (e) Validation of result.

Vendor Fraud Symptoms (Red Flags) and Its Risk

A red flag is a set of circumstances that are unusual in nature or vary from the normal activity. These are indicators that fraudulent activity could exist; they are not absolute, but

should be investigated to ensure fraudulent activity is not present. The red flags related to vendor fraud risks are presented in Table 1. These vendor red flags indicate that there is probability of commit a fraud by individual vendor or collision with vendors or collision among vendor and employee of the organisation or collision with vendor and customer as payment against fictitious materials/services or inflated invoices, etc.

Table 1: Red Flags Related to Vendor Fraud Risks

Vendor Red Flag	Risk for Vendor Fraud	Risk*
Incomplete Address	Fake Vendor, Shell Company Scheme, Phantom Bid, Ghost Vendor	Low
Abbreviated Vendor Names	Duplicate Vendor, Bid Rigging, Shell Company Scheme, Fictitious vendor	Low
In active vendors in system	Fictitious vendor	Low
One time vendor active in system	Fictitious vendor, Shell Company Scheme	Low
Sharing of the same address or phone number, TIN or other key data elements.	Duplicate Vendor, Nepotism	Low
Multiple "remit to" addresses.	Shell Company Scheme, Fake vendor, Flipping	High
Payments to contractors not on approved vendor list	Shell Company Scheme, Fake vendor	High
Vendors not located in business directories	Shell Company Scheme, Fake vendor	Low
Incorrect vendor Address	Shell Company Scheme,	Low
Multiple vendor address	Duplicate vendor	Low
Invoices for unspecified or poorly defined services or Vendor uses unfamiliar services	Shell Company Scheme, Substitution, Flipping	High
Unnumbered or sequentially numbered vendor invoices or Boilerplate contracts that have no clear definition of goods or services to be delivered	Shell Company Scheme, Fake vendor, Flipping	High
Vendor and employee have similar or identical information	Conflict of interest	High
Vendor fails to submit PAN or TIN	Fake Vendor, Shell Company Scheme	Low
Unexplained increase in volumes of purchases	Fake Vendor, Shell Company Scheme	High
Poor, illegible, or missing documentation supporting a vendor payment	Fake Vendor, Shell Company Scheme	High
Large billings broken into multiple smaller invoices that fall just below a threshold limit	Shell Company Scheme	High
An invoice with an even amount (round number) that is not expected or reasonable	Shell Company Scheme	Low
A check for an out-of-town vendor cashed locally	Shell Company Scheme	Low
An employee shows interest in invoices submitted by a particular vendor	Conflict of interest	High
Change in key field of vendor	Fake payment scheme, Flipping	High
Change in vendor master critical details followed by a change back to original after a short time and payment made in the interim period.	Flipping	High
Same vendor, amount and date but different invoice no.	Duplicate payment	High
Two Vendors with same invoice number, date and amount	Duplicate vendor or payment	High
Same invoice paid out of two different systems paid to a vendor.	Duplicate payment	High
Employees creating vendors, approving Purchase orders and processing invoices	Violation of segregation of duties	High

*Based on experience

Perpetration of Vendor Fraud

As discussed in Table 1, with the help of vendor red flags, we can easily identify occurrences of vendor frauds in term of fake vendor, fictitious vendor, shell company scheme (a shell company is a company that has no physical presence and generates little independent economic value), flipping (temporarily modifying an existing vendor), conflict of interest (officials involved in supply chain management have to act their duties in organisational interest. If they perform duties to gain any benefits to their family members or friends, it is conflict of interest), nepotism, phantom bid (the submission of fake quotation from

either real or fictitious vendors to make actual bids look more favourable), bid rigging (multiple vendors or suppliers agree to fix rate or other terms and conditions of purchase orders, such as to make a vendor a winner. The vendors may agree to rotate the next bid among them to share the profit. Kickbacks may involve from the winning vendor), substitution (supply of material or service with substation of specification as agreed in purchase order terms and conditions), and permanently modify an existing vendor and use of one-time account. These risk are generated due to activities in vendor master record by unapproved or incorrect changes, inappropriate use of the alternative payee function, vendor records not allocated to a reconciliation account, creation of duplicate vendor records, incorrect payments made through one-time vendor accounts, poor control of segregation of duties as authority of same person as vendor maintenance and bank reconciliation, vendor maintenance and purchase orders, vendor maintenance and vendor invoice/ payments etc.

Vendor Fraud Scenarios

A vendor fraud scenario may be defined by known vendor fraud, and collusion of employee and vendor, with the help of a list of transaction and attributes, rule, etc. Some of these vendor fraud scenarios are operated by individuals without any collision as discussed below:

Fake Vendor Scenario

Fake vendors may be created by fraudster in SAP using the t-codes XK01, MK01, and FK01 without making complete entry of the respected vendor's field. Payment to the vendor should be performed by F-40, F-44, F-48, and F-53. After payment to such vendors, there is no trace of these vendors or fraudster may delete entire field of such vendors from system by using t-code XK06 as shown in Fig. 2.

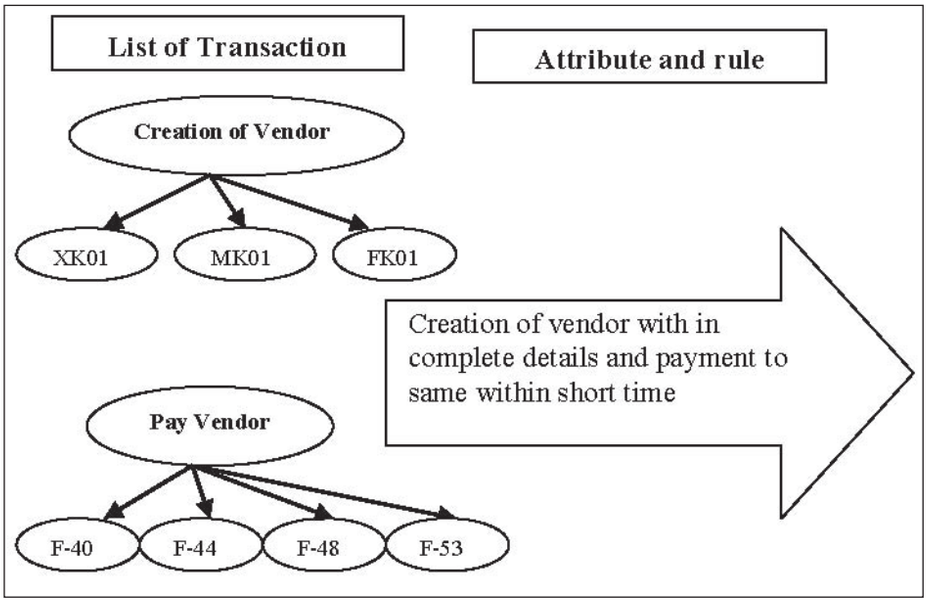

Fig. 2: Fake Vendor Scenario

Duplicate Vendor Scenario

Duplicate vendor is performed by fraudster with the creation of abbreviated vendor names, sharing of the same address or phone number, or other key data elements in vendor master. They use this duplicate vendor for bid rigging or phantom bid. Vendor in SAP can be created in system by using the t-codes XK01, MK01, and FK01 and payment to the vendor can be performed by F-40, F-44, F-48, and F-53. The payment to such duplicate vendors in short time may indicate the occurrence of such fraud as shown in Fig. 3.

List of Transaction Attribute and rule

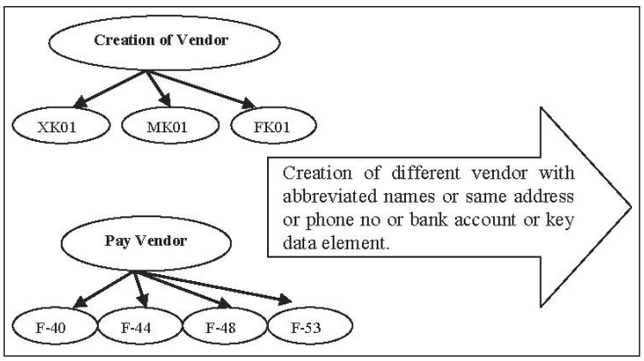

Fig. 3: Duplicate Vendor Scenario

Flipping Vendor Fraud Scenario

Flipping vendor fraud is performed by fraudsters through temporarily modifying an existing vendor master field such as bank account and redirecting the payment in the account of their choice instead of the vendor's actual account. After the payment is made, the fraudster changes the bank details back to the original values. Bank details of a vendor in SAP should be changed by using the t-codes XK02, FK02, FI01, and FI02 and payment to the vendor should be performed by F-40, F-44, F-48, and F-53. Change in vendor bank account field and a comparison with the payment to such vendor in short time may indicate the occurrence of such fraud as shown in Fig. 4.

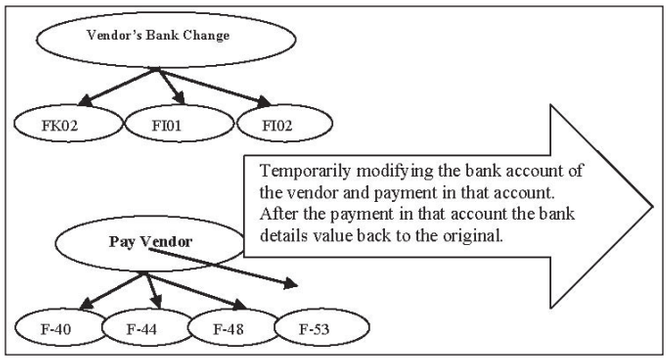

Fig. 4: Flipping Vendor Scenario

False Invoice Payment

The false invoice payment scenario is the creation, approval and payment of a false invoice. The false or fake invoice can be created in SAP system by use of any of the transaction codes FB60 of F-43 or MIRO and approval of this can be performed by MRBR transaction code. The last activity, making a payment, to the vendor of any kind is discussed in fake vendor or duplicate of filliping vendor scenarios. If the user has authority to create vendor, create invoice and make payment, then it can be easily performed. The above discussed activities are the violation of segregation of duties in the system as shown in Fig. 5.

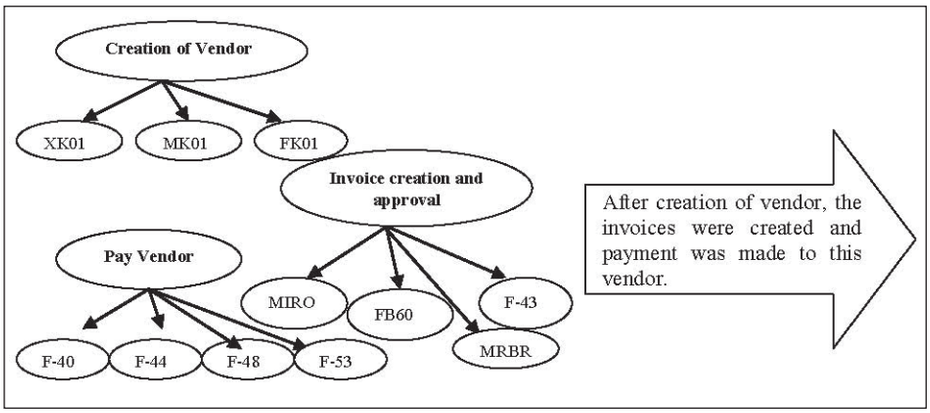

Fig. 5: False Invoice Payment Scenario

Non-Purchase Payment (Misappropriation)

The non-purchase payment with collusion is the generation of a purchase record in the system and a payment being made without the purchase actually occurring. The fraud may potentially exist when a user is authorised to create a purchase order by using t-code ME 51 and its approval by using ME58. Further the same person having authority of creation of goods received (t-code MIGO) and invoice verification. This is also a scenario of poor system control which gives opportunity to fraudster to violate segregation of duties and commit fraud and require further investigation shown in Fig. 6.

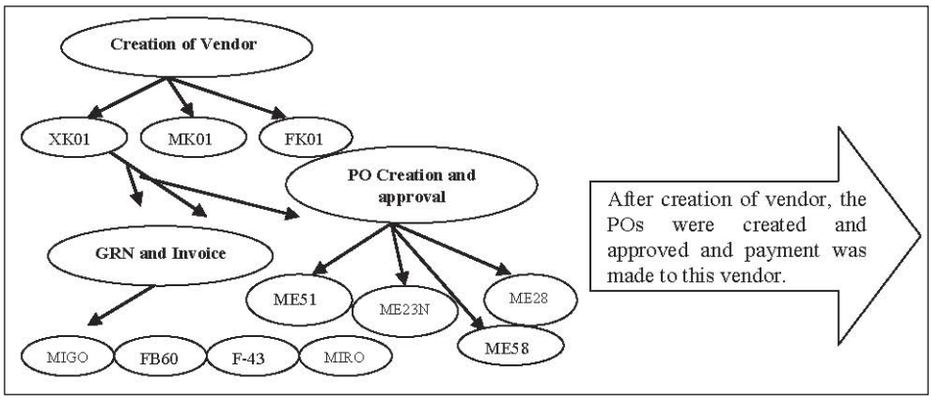

Fig. 6: Non-Purchase Payment Scenario

The extended vendor fraud scenarios which are created by collision of employee and vendor may identify with help of SAP vendor, employee and customer data, phone and email logs, and analyses them in context of above mentioned scenarios.

Vendor Fraud Detection: Methodology

The vendor master file in SAP is used to store information about vendors including the master records contain critical data elements, including the vendor bank account which is used for automatic payment and control key elements, such as whether the duplicate invoice check is performed for each individual vendor. Data is stored at three levels in the vendor master file and authorised user can create vendor in SAP R3 by transition code XK01 (centrally i.e. general data that relates to every company code and purchasing entity of vendors), MK01 (purchasing i.e. purchasing data, partner function that is used in the raising of purchasing documents), and FK01 (accounting data that is specific to each company code i.e. bank details, tax details etc) without any interlock. Changes can be done in SAP R3 by transition codes XK02, MK02, and FK02. Display can be done with help of XK03 t-code. Each function in SAP has a t-code (transaction code) which is a shortcut that takes the user directly to a SAP application rather than having to navigate through the menu system e.g. XK01- vendor creation and the performance of it is captured in audit trails. The audit trail data are stored in several tables as LFA1, some examples related to vendor were shown in figure 7a. Any changes in records are stored in two tables, CDHDR (Change Document Headers), and CDPOS (Change Document Items) Figure 7b

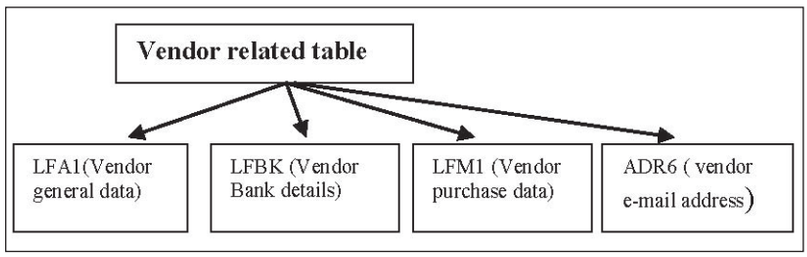

Fig. 7a: Vender Master Table

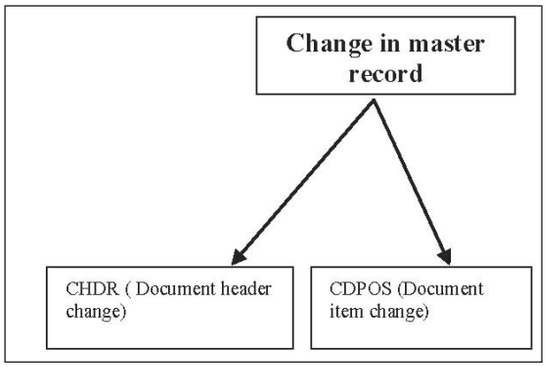

Fig. 7b: Change of Record Table

Accounting details are recorded in tables BKPF–Accounting Document Header, BSEG–Accounting Document Line Item and SKAT–General Ledger Account Texts. In any organisation, system may record huge numbers of transactions on daily basis and hence it is difficult to find a few instances of fraud. The FB01 transaction code allows the user to post any financial transaction including general ledger, customer, vendor, inventory, or asset transactions. The user enters a document type (e.g., SA, for GL postings) as part of the header data and then enters relevant data. Security guidelines usually recommend that no user be granted access to this transaction code; rather their profile should allow access to a set of specific transaction codes associated with their position (e.g., an accounts payable clerk). This user performed vendor maintenance, invoice entry, and payment processing

activities. Roles of all users mentioned above that have performed these activities require review and appropriate restrictions in SAP profiles. Another way to review security audit log which is extracted from SM20. These audit logs contains date, time, client, user-id, transaction code, terminal name, message identifier, and message text are retained until deleted. These functionalities can be used to detect fraudulent user behaviours.

Data

The transaction data is periodically extracted from related tables from SAP. In context of above discussion related to vendor fraud scenario, the data from SAP was extracted from the SUIM user authorities related to t-codes as discussed in fraud scenario. The users were identified and their roles compared to those who were creating conflicting roles in this organisations as shown in Table 2.

Table 2: User ID verse t-codes

User ID	XK01	MK01	FK01	XK02	MK02	FK02	FI01	FI02	F-40	F-44	F-48	F-53	FB01	FB60	MIGO	MIRO	ME51	ME58	ME23N	ME28	Fraud Probability
A00125	■			■						■			■								Y
A00127	■													■		■	■		■	■	Y
A00315				■			■				■										Y
B00971	■	■	■	■	■	■									■						Y
D00108	■															■		■			Y
00C222	■								■						■						Y
00C634		■			■		■								■	■					Y
01C004	■																	■			Y
F00004			■			■		■													Y
F_BASIS	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	Y

The above user ID employees were suspicious employee who has opportunity to commit vendor fraud. Hence, we had extracted security audit log by using SM20 code related to above user and filtered it on basis of use of vendor sensitive t-codes in abnormal day or time. Finally, the data for this specific period were extracted from tables LFA1 (vendor general data), LFBK (vendor bank data), CDHDR (change document headers), CDPOS (change document items), BKPF (accounting document headers), BSEG (accounting document line items) etc. These data were imported in excel sheets for analysis by using excel functions pivot tables, lookup, IF etc.

Data Analysis

On the basis of data extracted from SAP with help of t-code SM20, we found that the user F_BASIS had created a user F00041 and a vendor F14 at mid night on 05.01.2017. In the same time interval a new role and profile were generated by administrator and attached with new user F00041. User F00041 then apparently logged on to client 600 changing the initial password and used transaction FK02 to perform vendor maintenance. Finally, after posting any financial transaction through t-code FB01, the user ID post F00041 was deleted by user F-BASIS the same night. The activities are shown in Table 3.

Table 3: System Audit Log

Date	Time	Client	User	t- Code	Terminal Text
04.01.2017	16:55:04	600	A00103		Logon Failed (Reason = 1, Type = A)
04.01.2017	16:55:06	600	A00103		Logon Failed (Reason = 1, Type = A)
04.01.2017	16:55:23	600	A00103		Logon Failed (Reason = 1, Type = A)
04.01.2017	16:55:19	600	A00103		User A0103 Client 600 After Erroneous Password checks
04.01.2017	19:05:01	600	F_BASIS	SU01	Transaction SU01 Started
04.01.2017	19:05:02	600	F_BASIS		Unlocked After Being Locked Due to Inval. Password entered

Contd.

Date	Time	Client	User	t- Code	Terminal Text
05.01.2017	00:15:33	600	F_BASIS		Logon Successful (Type=A)
05.01.2017	00:16:16	600	F_BASIS	SU01	Transaction SU01 Started
05.01.2017	00:21:38	600	F_BASIS	SU01	User F0041 Created
05.01.2017	00:21:39	600	F_BASIS	SU01	Authorizations for User F0041 Changed
05.01.2017	00:28:34	600	F_BASIS	SU03	Transaction SU03 Started
05.01.2017	00:31:19	600	F_BASIS	SU03	Authorization Z:AUTH5001/F_KNA1_BUK Activated
05.01.2017	00:31:25	600	F_BASIS	PFCG	Transaction PFCG Started
05.01.2017	00:33:05	600	F_BASIS	SUPC	Transaction SUPC Started
05.01.2017	00:36:23	600	F_BASIS		Authorization Z:VENDF14_00/ F_BKPF_BEK Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_BKPF_BLA Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_BKPF_BUK Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_BKPF_GSB Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_BKPF_KOA Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_LFA1_AEN Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_LFA1_APP Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_LFA1_BEK Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_LFA1_BUK Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_LFA1_GEN Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/ F_LFA1_GRP Activated
05.01.2017	00:36:24	600	F_BASIS		Authorization Z:VENDF14_00/S_TCODE Activated
05.01.2017	00:36:24	600	F_BASIS		Profile Z:VENDF14_ Activated
05.01.2017	00:37:15	600	F_BASIS	SU01	Transaction SU01 Started
05.01.2017	00:37:47	600	F_BASIS	SU01	User Master Record F00041 Changed
05.01.2017	00:37:48	600	F_BASIS	SU01	Authorizations for User F00041Changed
05.01.2017	00:38:20	600	F00041		Logon Successful (Type=A)
05.01.2017	00:38:21	600	F00041		Password changed for user F00041 in client 600
05.01.2017	00:39:00	600	F00041	FK02	Transaction FK02 Started
05.01.2017	00:40:07	600	F00041	FB01	Transaction FB01 Started
05.01.2017	00:59:38	600	F00041		User Logoff
06.01.2017	01:09:02	600	F_BASIS		Transaction SU01 Started
06.01.2017	01:11:08	600	F_BASIS		User F0041 Deleted
06.01.2017	01:13:01	600	F_BASIS		User Logoff

On analysis of activity shown in Table 3, it was found that user F_BASIS had created fake vendor and make payment in name of this shell company. Hence there was a chance of other fraudulent activities by F_ BASIS user. On analysis of vendor changes, it was observed that vendor CA14 was modified by F-BASIS on holiday of the organisation (02.10.2016) by changing its bank account to 320846222903. On 25.12.2016 the bank account was restored to original values, 110000004501 as before 02.10.2016 by F-BASIS user. This analysis was carried out with help of two tables of SAP, CDHDR (change document headers) shown in Table 4 and CDPOS (change document items) shown in Table 5, where these changes were stored. Further, it was observed that user had utilised XK02 t-code, to change the bank account.

Table 4: Change Log against Vendor CA14

MANDANT	OBJECTCLAS	OBJECTID	CHANGENR	USERNAME	UTIME	TCODE	UDATE
600	KRED	CA14	187577668	F_BASIS	02.10.2016	XK02	23:40:00
600	KRED	CA14	275471416	F_BASIS	25.12.2016	XK02	00:02:09

Table 5: Change Log against Object ID CA14 and Change ID 187577668

MANDANT	OBJECTCLAS	OBJECTID	CHANGENR	TABNAME	TABKEY	FNAME	CHNGIND
600	KRED	CA14	187577668	LFA1	600CA14	CONFS	U
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 110000004501	KEY	I
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	BKONT	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	BKREF	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	BVTYP	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	EBPP_ ACCNAME	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	EBPP_ BVSTATUS	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	KOBIS	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	KOINH	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	KOVON	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_NEFT 320846222903	XEZER	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 110000004501	KEY	I
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	BKONT	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	BKREF	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	BVTYP	E

Contd.

MANDANT	OBJECTCLAS	OBJECTID	CHANGENR	TABNAME	TABKEY	FNAME	CHNGIND
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	EBPP_ ACCNAME	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	EBPP_ BVSTATUS	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	KOBIS	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	KOINH	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	KOVON	E
600	KRED	CA14	187577668	LFBK	600CA14 IN EPAY_RTGS 320846222903	XEZER	E

where U- Update, I- Insert, and E- Delete (Single Field Documentation)

On the basis of above analysis, it was clear that user F-BASIS had used vendor flipping sceneries. Then by using BKPF accounting document headers a document number 1000000201 was observed in table on 04.11.2016 against the vendor CA14. In BSEG accounting document line items table, there were three debit/ credit entries corresponding to this document. Every posting to a general ledger reconciliation (control) account also specifies the relevant subsidiary ledger record (table SKAT). Account number 209000 is the accounts payable account as general ledger account texts (names) are stored in table SKAT. The accounting document headers and line items indicate the suspects and invoice and payment transactions for the associated vendor, CA14. The invoice (using FB60) posted by F_BASIS user on 04.11.2016 was for Rs. 400000 to vendor CA14. Payment occurs on 24.11.2016; it appears that F_BASIS have successfully perpetrated a vendor fraud by using changed banking details by flipped back.

Result and Discussion

On the basis of security audit log, tables related to vendor master and payment, it was revealed that the user F_ BASIS had performed fraudulent activity. The F_BASIS user was system administrator of SAP system for this organisation, who is not related for functional activities. But he had created opportunity in help of weak control and monitoring of system to commit fraud. On analysis of the data generated in name of this user ID for past one year, the following was found:

The unlimited accesses to system functions of user F_BASIS was assigned like the profile designed in SAP_ALL.

Initially more than two thousand vendor records were uploaded in SAP system from legacy system by using the user ID F_BASIS.

This user had the authorities of creation and modification of vendor, creation of purchase requisition & purchase orders and its approval, creation of invoice and payment etc. which was the violation of segregation of duties.

This user had created more than 10 vendors, in which one vendor had incomplete data and one vendor's address and account details were in name of his brother in law in year 2014. But there was no any payment activities made in name of these two vendor codes. It indicates that the attitude of user F_BASIS was not fair.

The bank accounts of 3 vendors were also changed by this user in name of a relative during the period of this fraud identify, and the payments of value approx. Rs. 25 lacs were diverted in the changed account.

The user F_BASIS had applied the vendor fraud as creation of fake vendor, fictitious vendor, shell company scheme, flipping, conflict of interest, nepotism, etc. On further analysis, it was also observed that an invoice was paid to the account of a vendor, which has the same bank details as another vendor in the system.

This was a red flag as duplicate vendors were found in this system. It seemed that the users shown in table are

performing the functions as maintaining vendors, creating purchase orders and its approval, entering invoices and paying vendors. There were breaches in the normal segregation of duties principles.

Limitations

The behaviour of individual users will be recorded in detail in the audit trails log in SAP system. As the user F_BASIS had privilege of 'super-users' of unlimited privileges, he was able to selectively edit audit trail data, such as entries in the security audit log, to remove evidence of 'red flags' associated with their own activities. Similarly, internal and external intruders in the system who are masquerading as authentic users may target these super-users and exploit these capabilities to remove any trace of their activities in the system.

Conclusion

A number of fraud cases have shocked the economic markets in the recent past and it is an emerging global problem in private and public organisations. The vendor fraud is a major component of supply chain fraud. The detection and prevention of vendor frauds are challenging for the organisations, because of the adoption of new strategies committed by fraudsters. For detection of vendor fraud, it requires in-depth knowledge about the nature, modus operandi for auditing, investigating agencies responsible for corporate governance. This paper has been demonstrated in easy way for vendor fraud detection proactively with help of audit system log and data stored in the SAP tables related to vendor master and payment. Corporate governance agencies of organisations may detect the vendor fraudulent activities with the help of the steps mentioned above. In future this can be performed by data mining tools and text mining. One important challenge is how to integrate continuous fraud detection in the SAP system.

Reference

ACFE. (2014). Report to the nation on occupational fraud and abuse. Retrieved from http://www.acfe.com/rttn

Albrecht, W. S., Albrecht, C. C., Albrecht, C. D., & Zimbelman, M. (2009). *Fraud Examination* (3rd Ed.). Thomson/South-Western, Mason OH.

Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems*, 7(2), 137-161.

Best, P. J., Rikhardson, P., & Toleman, M. (2009). Continuous fraud detection in enterprise systems through audit trail analysis. *Journal of Digital Forensics, Security and Law,* 4(1).

Broady, D. V., & Roland, H. A. (2008). SAP GRC for dummies. Retrieved from http://library.books24x7.com.ezproxy.usq.edu.au/toc.asp?bkid=25161 Coderre, D., & Warner, P. D. (1999). Computer-asisted techniques for fraud detection. *CPA Journal*, 69(8), 57.

Cressey, D. R. (1953). *Other people's money: A study of the social psychology of embezzlement.* New York, NY US: Free Press.

Debreceny, R. S., Gray, G. L., Jun-Jin Ng, J., Siow-Ping Lee, K., & Yau, W. F. (2005). Embedded audit modules in enterprise resource planning systems: Implementation and functionality. *Journal of Information Systems*, 19(2), 7-27.

Edge, M. E., & Falcone Sampaio, P. R. (2009). A survey of signature based methods for financial fraud detection. *Computers & Security,* 28(6), 381-394.

Islam, A., Corney, M., Mohay, G., Clark, A., Bracher, S., Raub, T., & Flegel, U. (2010). *Fraud detection in ERP systems using scenario matching.* Proceedings of the Twenty-Fifth IFIP International Conference on Information Security, 112-123.

Little, A. G., & Best, P. J. (2003). A framework for separation of duties in an SAP R/3 environment. *Managerial Auditing Journal*, 18(5), 419-430.

Narayan, V. (2008). *Financial Accounting (FI)*. SAP FI/CO questions and answers. Sudbury: Infinity Science Press.

O'Gara, J. D. (2004). *Corporate fraud case studies in detection and prevention.* Hoboken, NJ: Wiley & Sons.

Padhi, S. N (2010). *SAP ERP financials and FICO handbook*. Burlington, MA: Jones and Bartlett.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). *A com prehensive survey of data mining-based fraud detection research*. arXiv 1-14.

Potla, L. (2003). Detecting accounts payable abuse through continuous auditing. *IT Audit,* 6(3). Retrieved from http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5458.

Singh, K., & Best, P. J. (2015). Design and Implementation of Continuous Monitoring and Auditing in SAP Enterprise Resource Planning. *International Journal of Auditing,* 19, 307-317. doi:10.1111/ijau.12051

Singleton, T., Singleton, A., Bologna, J., & Lindquist, R. (2008). *Fraud auditing and forensic accounting*. Hoboken, NJ: John Wiley & Sons.

Srinidhi, B. (1994). The influence of segregation of duties on internal control judgements. *Journal of Accounting, Auditing & Finance,* 9(3), 423-444.

Wells, J. T. (2002a). Billing schemes, part 1: Shell companies that don't deliver. *Journal of Accountancy*, 194(1), 76-79.

Wells, J. T. (2008). *Principles of fraud examination* (2nd Ed.). Hoboken, NJ: John Wiley & Sons.

Wells, J. T. (2011). *Principles of fraud examination* (3rd Ed.). Hoboken, NJ: John Wiley & Sons.