Accounting and Management Information Systems
Vol. 19, No. 1, pp. 379-404, 2020
DOI: http://dx.doi.org/10.24818/jamis.2020.02008

Implementing Benford's law in continuous monitoring applications

Kishore Singh[a,1] and Peter Best[a]

[a] *Central Queensland University, Australia*

Abstract

Research Question: Do modern ERP systems record sufficient information to allow retrospective monitoring of accounts payable transactions? Can Benford's Law be applied to these transactions to detect potential fraud in accounting data? ***Motivation:*** Modern ERP systems are capable of recording several thousands of transactions daily. This makes it difficult to find a few instances of anomalous activities among legitimate transactions. As organizations continue to become more complex and demand more integrated business processes, automated analytics may provide auditors and fraud examiners some degree of assurance on continuous information simultaneously with, or shortly after disclosure of information. ***Idea:*** In this study we develop a proof of concept prototype to monitor invoice transactions and identify those that violate Benford's law. The prototype exploits audit trails in enterprise systems. ***Data:*** Data was obtained from the SAP ERP systems of two large organizations. Organization 1, a government department, provided a one month sample of accounting transaction data. Organization 2, a global manufacturing company, provided a six month sample of their transaction data. ***Tools:*** Verification and validation was achieved by obtaining independent reviews from an expert and a panel of auditing practitioners. Their feedback was sought using a survey instrument where they rated various aspects of the prototype software. ***Findings:*** A key aim was to demonstrate the feasibility of implementing Benford's analysis in continuous monitoring applications by exploiting audit trails in ERP systems. The concept was demonstrated by designing prototype software. We found that Benford's analysis, is a useful tool for identifying suspicious transactions. These transactions may contain possible errors, potential fraud or other irregularities. ***Contribution:*** An important contribution of the study is that the entire population of transactions for a specified time period are analyzed. This

[1] *Corresponding author:* Kishore Singh, Senior Lecturer, Central Queensland University, 160 Ann Street QLD 4000, Australia, e-mail: k.h.singh@cqu.edu.au

approach is in contrast with the traditional or manual audit approach which is limited because it reviews only a small percentage of a large population of transactions. The prototype demonstrates the application of technology and data analytics to process transaction data from a SAP ERP system in a near real-time basis. This represents the next step in the evolution of the financial audit from manual to automated methods.

Keywords: Benfords Law, fraud, accounts payable, SAP audit trail analysis, internal audit

JEL categories: M41, M42

1. Introduction

In 1881, astronomer and mathematician Simon Newcomb (1881) casually observed that the first pages in books of logarithmic tables appeared to wear out much faster than the last ones. People appeared to look up numbers with digits 1 and 2 more often than numbers beginning with digits 8 and 9. Based on his observation, Newcomb concluded that in a sequence of positive real numbers, assuming that the mantissas of their logarithms are equally probable, it is possible to determine the percentage of the numbers whose first digit is 1 up to 9. Similarly, it is possible to determine the percentages of the second digit (from 0 to 9), and so on up to *n*-th digit. Frank Benford, an engineer and physicist set out to empirically test Newcomb’s hypothesis. He collected a variety of datasets including population figures, addresses, newspaper items, death rates, baseball statistics, atomic weights of elements, and numbers appearing in Readers Digest articles among others (Benford, 1938). His analysis found a good fit to the distribution of first digits determined by Newcomb. This phenomenon became known as Benford’s law. Accordingly, whilst human intuition is that each number in a collection has equal opportunity of appearance, Benford’s law reports that the digit 1 leads approximately 30% of the time, and the frequency of each subsequent digit reduces, with digit 9 occurring in less than 5% of the cases.

Modern enterprise systems are capable of recording several thousands of transactions daily. This makes it difficult to find a few instances of anomalous activities among legitimate transactions. For large organizations operating in an evolving global digital marketplace, this means monitoring hundreds of thousands of transactions and investigating suspicious ones in-depth. This may involve considerable expense (Singh *et al.*, 2014). A typical organization loses approximately 5% of its annual revenue to fraud (ACFE, 2016b). A large proportion of victim organizations are unable to recover their losses from fraudulent activity hence proactive measures to prevent and detect fraud are imperative. Consequently, the need for continuous auditing and continuous monitoring (CACM) has increased in the global digital economy as organizations become more complex and demand more integrated business processes (Vasarhelyi *et al.*, 2010).

Verification and validation of the prototype were conducted to check that software systems met specifications. Verification was conducted using test data involving simulated transaction activity. Validation was achieved by obtaining independent reviews from an expert and a panel of auditing practitioners. The Executive Director of Information Systems Audit of a top international accounting firm reviewed the software. He conducted internal audit tests using his firm's data *(results withheld due to confidentiality*). Feedback was also from an expert panel of auditing practitioners.

In this study the authors develop a proof of concept prototype to monitor invoice transactions and identify those that violate Benford's law. The prototype examines audit trails obtained from accounting information systems to establish whether it is feasible to identify invoices with irregular characteristics (Singh, 2012[2]). These designs highlight the application of technology and data analytics to process accounting transaction data as they occur using predetermined rules or signatures (Kuhn Jr and Sutton, 2010). The intention is to provide compliance personnel with a level of assurance as transactions are processed (Rezaee *et al.*, 2002, 150). This represents the next step in the advancement of the financial audit from traditional manual methods to automated methods (Vasarhelyi *et al.*, 2012). These systems are only feasible because they are fully automated with instantaneous access to accounting transactions (Kogan *et al.*, 1999).

The study uses design science as its methodological framework (Hevner *et al.*,2004). The framework consists of the following key steps, namely, i) creation of an innovative artifact for solving a specific problem, ii) the solution to the problem must be effective iii) the artifact must be thoroughly evaluated and, iv) findings must be presented to both technology- and management-oriented audiences. As the focus of this study is on developing proactive techniques for detecting potentially fraudulent transactions in accounts payable in SAP ERP systems, the following two research questions are investigated (Singh, 2012):

- RQ1: Do SAP audit trails document adequate data to allow retrospective monitoring of accounts payable transactions?
- RQ2: How can Benford's analysis be implemented in continuous monitoring applications to detect anomalous accounting transactions?

[2] This article is based on research conducted in the corresponding authors PhD. Consequently, many empirics and results come from there.

A key contribution of the study is to demonstrate the feasibility of implementing Benford’s analysis in continuous monitoring applications using the entire population of accounting transactions for a specified time period are analyzed. This approach is in contrast with the traditional or manual audit approach which is limited because it reviews only a small percentage of a large population of transactions. The prototype demonstrates the application of technology and data analytics to process transaction data from a SAP ERP system in a near real-time basis. This represents the next step in the evolution of the financial audit from manual to automated methods. We are therefore able to conclude that Benford’s analysis is a useful tool for identifying suspicious transactions which may contain possible errors, potential fraud or other irregularities in transaction data.

The paper is organized as follows: section 2 discusses the theoretical constructs of Benford’s law, section 3 describes the literature related to Benford’s law and section 4 describes the methodology adopted by the study. In section 5, the findings are discussed, followed by some limitations of the study and concluding remarks in section 6.

2. Benford’s Law

It has been observed that the first pages of a table of common logarithms show more wear than do the last pages, indicating that more used numbers begin with the digit 1 than with the digit 9 (Newcomb, 1881; Benford, 1938). Benford compiled over 20,000 first digits taken from a variety of widely different sources. Sources ranged from purely random numbers to formal mathematical tabulations. Analysis of these numbers revealed that there is a logarithmic distribution of first digits when the numbers are composed of two or more digits. Numbers taken from unrelated subjects demonstrate a much better fit with a logarithmic distribution than do numbers from mathematical tabulations or formal data. The distribution of first $(D_{1)}$, second (D_2), and first two digits (D_1D_2) in these data may be closely approximated by the following logarithmic distribution (Nigrini and Mittermaier, 1997)

$$P(D_1 = d_1) = log_{10}\left(1 + \tfrac{1}{d_1}\right)\ d_1 \in \{1, \dots 9\} \quad (1)$$

$$P(D_2 = d_2) = \sum_{d_1=1}^{9} log\ _{10}\left(1 + \frac{1}{d_1 d_2}\right)\ d_1 \in \{1, \dots 9\}\ d_2 \in \{0, 1, \dots 9\} \quad (2)$$

$$P(D_1D_2 = d_1d_2) = log_{10}\left[1 + \left(\sum d_i\ 10^{k-i}\right)^{-1}\right]\ d_1d_2 \in \{10, 11, 12\ \dots 99\} \quad (3)$$

where *P* represents the expected probability of the digit in parenthesis. Using equation 3, the expected probability of the first-two digits 75 would be calculated as follows:

$$P(D_1D_2 = 75) = \log_{10}\left(1 + \left(\frac{1}{75}\right)\right) = 0.005752 \quad (4)$$

The expected distributions for digits in the first, second, third, and fourth positions are shown in Table 1. It may be noted that the distribution of higher-order digits increasingly approximates the uniform distribution. It follows that when dealing with numbers with three or more digits than the rightmost digits are expected to be evenly distributed.

Table 1. Benford's Law Expected Digit Distributions

D_i	$P(D_1)$	$P(D_2)$	$P(D_3)$	$P(D_4)$
0	-	0.11968	0.10178	0.10018
1	0.30103	0.11389	0.10138	0.10014
2	0.17609	0.10882	0.10097	0.10010
3	0.12494	0.10433	0.10057	0.10006
4	0.09691	0.10031	0.10018	0.10002
5	0.07918	0.09668	0.09979	0.09998
6	0.06695	0.09337	0.09940	0.09994
7	0.05799	0.09035	0.09902	0.09990
8	0.05115	0.08757	0.09864	0.09986
9	0.04576	0.08500	0.09827	0.09982

(*Source*: Nigrini & Mittermaier, 1997)

Benford (1938) noted that the observed probabilities were closely related to events rather than the natural number system. Humans are accustomed to labelling things as 1, 2, 3, 4, … The idea that 1, 2, 4, 8, … being a more natural arrangement is not readily accepted. However, the latter occurs in an unexpectedly large number of phenomena, for example, the growth of the sensation of brightness with increasing illumination, or the sense of loudness are two instances of logarithmic functions. Benford further noted that some of the best fits to the logarithmic pattern was for data in which the numbers had no relationship to each other. Furthermore, the distribution does not occur if the observed values are from a small range, if the numbers are assigned, or fabricated by people (Slijepcevic and Blaskovic, 2014). This lead to the conclusion that the logarithmic relation is a Law of Anomalous Numbers (Benford, 1938).

The fact that a series of random numbers conforms to Benford's law suggests that its application is suitable for detection of fraudulent data in accounting transactions (Nigrini and Mittermaier, 1997; Durtschi *et al.*, 2004; Ciaponi and Mandanici, 2015). By comparing expected frequencies of digits in invoice or payment transactions; unusual spikes may be indicative of fraudulent transactions and require further investigation by audit personnel.

Many fraudsters fail to consider the Benford’s Law pattern when creating false invoices or payments. Consequently, analyzing data sets for the occurrence or non-occurrence of the predictable patterns may uncover instances of asset misappropriation such as shell company schemes, fictitious billing schemes, inventory misuse or larceny, skimming or cash larceny and bill-splitting or other schemes involving circumventing predetermined transaction limits (Lanza, 2003; ACFE, 2016a). This study automates Benford’s Law to monitor and analyze accounts payable transaction data for anomalies or ‘red flags’ in invoice and payment transactions.

3. Related literature

Camerer (2003) proposed that people do a poor job of replicating known data-generating processes, for instance by over-supplying modes or under-supplying long runs. Hill (1988) provided experimental evidence that individuals cannot behave truly randomly and when asked to generate numbers, these numbers did not conform to Benford’s law. Although Benford's law is widely applicable to a variety of numerical data, it is not widely known (Tam Cho and Gaines, 2007). It is therefore reasonable to assume that those manipulating numbers would not seek to preserve fit to the Benford distribution, implying that it may be an unusually good tool to detect fraud, at least until it becomes widely known.

Several applications of Benford's law have been developed. Whenever first digits are expected to follow Benford's law, it follows that deviations from the known distribution signal the existence of potential fraud. Benford's law has subsequently been used as an effective tool to test for fraudulent manipulation of data. Thomas (1989) discovered excess second-digit zeros in net income data in the USA. He also examined earnings per share (EPS) and found unusual proportions of EPS numbers divisible by ten cents and five cents for firms reporting profits, but not for firms reporting losses. This result coincided with the Enron debacle and an analysis of ENRON numbers for 1997 to 2000 showed an excess of second-digit zeros (Nigrini, 2012). Christian and Gupta (1993) used Benford’s law to analyze taxpayer data to identify signs of tax evasion where taxpayers reduce their taxable income from a higher tax bracket to a lower one. Even a small reduction of a few dollars may lead to a large tax saving, especially at the margin of a tax bracket. They used Benford’s law to justify that the ending digits of taxable income should be uniformly distributed over the range 00 to 99.

Nigrini (1994) investigated whether Benford’s law was applicable to detecting fraud. Using data from a payroll fraud case, Nigrini conducted Benford’s analysis on the first two digits. Results showed that during the period that the fraud occurred, a significant deviation in Benford’s law was observed. Furthermore, in the latter period of the fraud case, deviations were at their peak, suggesting that the fraudster did not bother to invent authentic numbers. Tam Cho and Gaines (2007) cautioned that not all numbers follow Benford's law, for example, selling a large number of identical items whose price is constant may result in a skewed distribution of first digits. However, if distributions are randomly selected and random samples are taken from each distribution, the resulting dataset becomes compliant with Benford's distribution (Singh, 2012). Nigrini and Miller (2009) introduced a second order test related to Benford's Law that could be used for the detection of fraud, errors, and fabricated data. This second order test diagnoses the internal structure of the data. For many different types of data sets, if the observations are arranged in ascending order, then the numeric difference between successive digits conforms to Benford's Law. They demonstrated this second order test using three cases.

Durtschi *et al.* (2004) lists a series of guidelines relating to datasets that are expected to comply with Benford's law, namely, i) mathematical combinations such as quantity x price, ii) accounting transactions such as purchases and sales) and, iii) large datasets. In general, analyzing an entire dataset yields better results than when analyzing a sample. Conversely, not all datasets conform to Benford's. These may be classified as: i) allocated numbers such as invoice numbers), ii) manipulated numbers, for example, prices set at a threshold such as $1.99 and, iii) accounts set up for specific purposes, for example, accounts set up to record $100 refunds. Restrictions apply to many data sources, and consequently comparison to Benford's distribution is not always justified.

The use of Benford's law is in keeping with the philosophy of data mining where large volumes of data are searched for patterns. If a data source largely conforms to the law, random deletion would not induce a worse fit. However, if entries are being falsified, as in the case where embezzlement, or omissions have occurred, violations may be observed (Nigrini, 1999; Durtschi *et al.*, 2004) Given the number and variety of processes that produce Benford's distributed data, it is usually assumed that the first, second and later significant digits in real numerical data adhere to Benford's law. Additionally fabricated or falsified data has been tested for deviation from Benford's distribution in several studies. Some have reported success in identifying fraudulent information in tax or other financial data against the Benford distribution (Carslaw, 1988; Berton, 1995; Nigrini, 1996) and for falsified survey interviews (Schraepler and Wagner, 2005). Other diverse studies include election campaign finance (Tam Cho and Gaines, 2007), toxic gas emission (De Marchi and Hamilton, 2006) and data misrepresentation in mutual fund reporting (Zheng *et al.*, 2017).

Trompeter and Wright (2010) examined auditor experiences in the use of analytical procedures (APs). They determined that APs are powerful in detecting misstatements. They found that the Sarbanes-Oxley Act and recent scandals are important drivers of change in using APs. Furthermore, changes in technology and audit firm approaches have facilitated such change. Their study suggests that future work is needed to determine how auditors integrate information and whether structured tools may aid the process. Da Silva and Carreira (2012) contributed to digital analysis by formulating alternative models for selection of audit samples when performing Benford’s analysis. Their model allows an auditor to identify a subset of nonconforming records in a dataset. Their audit samples are chosen on a purely numerical basis.

Messier Jr *et al.* (2012) reviewed two decades of behavioral research on analytical procedures (APs) to inform their understanding of how APs performed in practice. Their review emphasized the need for more research on the use of APs during the audit. Hogan *et al.* (2008) identified the use of technology-based tools in auditing (namely; data mining, continuous auditing and pattern recognition) as an area of research that may help improve the efficiency and effectiveness of audits. Another area mentioned is the use of a risk-based approach in detecting fraud and investigating the effectiveness of internal controls. Brown *et al.* (2007) concluded that as business processes become more interlinked through the use of information technology, continuous monitoring will become a key assurance mechanism. Other contributing factors creating demand include the Sarbanes-Oxley Act and the need for frequent reliable financial disclosures. They determined that future work is needed to expand existing concepts relating to continuous monitoring and further empirical evidence is needed from actual implementations. More case studies documenting the types of audit algorithms, steps in implementation and factors contributing to successes may make significant contributions to the literature. Consequently, the objective of this study is to automate and apply Benford’s distribution to invoice transactions by effecting continuous monitoring principles. In this study the entire population of transactions for a specified time period are analyzed. This approach is in contrast to the traditional or manual audit approach which is limited because it reviews only a small percentage of a large population of transactions. The aim is to confirm the feasibility of implementing proactive detection of anomalous invoices in practice by using Benford’s Law.

4. Methodology

The principal objective of this study is to demonstrate the feasibility of implementing Benford’s analysis in continuous monitoring (CM) applications to detect anomalous accounting transactions. Accordingly, the study adopts Hevner, et. al’s (2004) design science methodological framework. The framework requires creation of an innovative, purposeful artifact for a specified problem domain. Evaluation of the artifact is crucial. The artifact must be innovative and thoroughly designed and evaluated. It must enact an effective solution to a problem space and results of the research must be presented effectively to both technology- and management-oriented audiences. This study aligns with Hevner, *et al.*’s (2004) framework as follows: 1) related literature – to recognize theories and concepts that support the study, 2) identifying data requirements to detect Benford’s Law anomalies in an SAP Enterprise System, 3) designing, developing and implementing a prototype, 4) performing tests to verify functionality of the prototype, and 5) seeking support from experts for validation of the prototype.

4.1 Aim of study

The aim of the study is to explore and develop innovative methods to implement Benford’s analysis in CM applications for detection of fraudulent invoices based on analysis of patterns of dollar amounts. The approach is to exploit audit trails in enterprise systems. The concept is demonstrated by designing prototype software to confirm the feasibility of implementing Benford’s analysis in practice. The software analyses high-volume transaction data from a SAP enterprise system for ‘red flags’ of invoice and payment fraud. Reports and charts highlighting anomalous activities are produced. Charts are diagrammatic representations of a data set. They assist a reader to easily interpret discrete or continuous data. The information usually determines the presentation method, for example, a continuous line chart implies that values can be taken at any point on the line. Conversely, discrete data is more suited to being plotted using a bar or column chart (Kim *et al.*, 2006). This study uses bar charts to demonstrate conformity of invoice amounts to Benford’s law. We focus in our analysis on transaction data obtained from the ERP systems of real organizations. This data is used to analyze invoice and payment transactions for violations of Benford’s law. Further investigation of anomalies is at the discretion of audit and compliance personnel.

Given the pervasiveness of enterprise systems research is necessary to advance the awareness, relevance, and practicality of continuous detection of potential fraud that uses technology to rapidly analyse large sets of transaction data (Debreceny *et al.*, 2005; Singleton and Singleton, 2007; Kuhn Jr and Sutton, 2010). It appears that prior research on continuous auditing does not appear to deliver a model that facilitates proactive and continuous monitoring for potential fraud without difficulties. Research is especially required in developing approaches of continuous monitoring that are specifically applicable to auditing of financial transactions in enterprise systems (Debreceny and Gray, 2010; Kuhn Jr and Sutton, 2010; Kotb and Roberts, 2011). Most organizations conduct their business activities online and in real-time. This necessitates continuous monitoring which enables internal auditors to perform their analyses of key business systems in real- or near real-time (Kogan et al., 1999; Alles *et al.*, 2002; Rezaee et al., 2002; Coderre, 2005; Alles *et al.*, 2006; Kuhn Jr and Sutton, 2010; Kotb and Roberts, 2011).

4.2 Research Questions

The focus of this study is therefore on developing proactive techniques for detecting potentially fraudulent transactions in accounts payable in SAP enterprise systems. Actual fraud can only be confirmed these activities are fully investigated. Thus, the following two research questions are investigated:

RQ1: Do SAP audit trails document adequate data to allow retrospective monitoring of accounts payable transactions?

The primary source of data for detection of fraudulent invoices in accounting systems, in general, is the invoice payment file. In particular, the following information is essential: vendor name, invoice number, invoice date, posting date, payment date, amount and user that processed the transaction. In SAP enterprise systems, audit trails provide detailed descriptions of functions performed within the system. Each function in SAP has a transaction code associated with it. A transaction code (or t-code) consists of letters, numbers, or both (for example, FB60 – Enter Vendor Invoice). Each transaction code executed by a user is recorded in an audit trail (Best, 2000). Audit trail data required for this research is stored in several tables within a SAP enterprise system. Accounting audit trails are stored in tables BKPF – Accounting Document Header, BSEG – Accounting Document Line Item, SKAT – General Ledger Account Texts, and LFA1- Vendor General Data. Tables BKPF and BSEG store posting histories for both general ledger accounts and subsidiary ledger records. This facilitates integration of data and automatic reconciliation of subsidiary ledgers with control accounts. General ledger account texts (names) are stored in table SKAT. Vendor general data including vendor name, date created and creating user are stored in table LFA1 (Best *et al.*, 2009). Thus it is possible to identify an individual user performing these activities.

As noted in the preceding discussion, data describing accounting transactions activities is well-documented in audit trails of a SAP enterprise system. Analyzing and identifying high-volume accounts payable transactions for anomalies, however, is not easily accomplished.

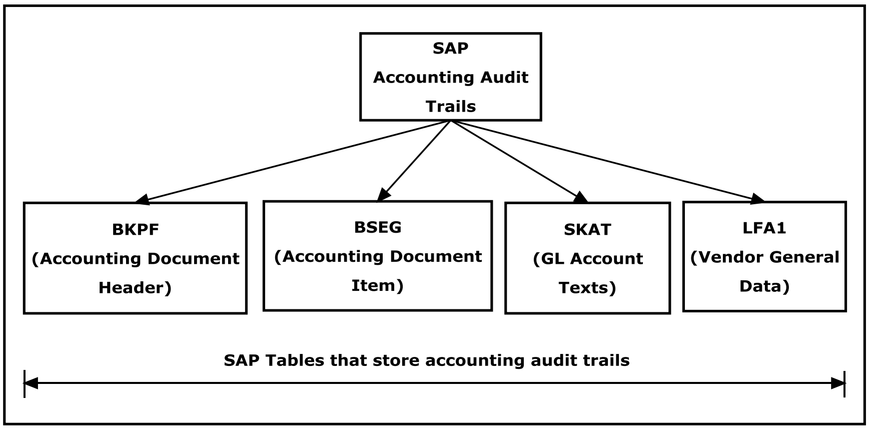


Figure 1. SAP Enterprise System Accounting Audit Trails

RQ2: How can Benford's analysis be implemented in continuous monitoring applications to detect anomalous accounting transactions?

There are two key advantages for constructing software prototypes that are relevant to this study: i) to provide users with a 'tangible' idea of the problem solution being sought after; and ii) to demonstrate the technical feasibility of a specification (Budde and Zullighoven, 1990; Asur and Hufnagel, 1993). Thus, the purpose of the prototype sub-system, is to demonstrate the feasibility of implementing Benford's analysis in practice. It provides evidence in support of the research question, i.e. it demonstrates how this strategy can be implemented, though it is only a 'proof of concept' tool, not a commercial application for use by auditors and other end-users.

Data requirements for anomaly detection in SAP enterprise systems are discussed above. Accounting audit trails are routinely extracted from a SAP enterprise system, cleansed (to remove any inconsistencies) and pre-processed (which ensures only invoices and payments are extracted), prior to processing and analysis (Figure 2).

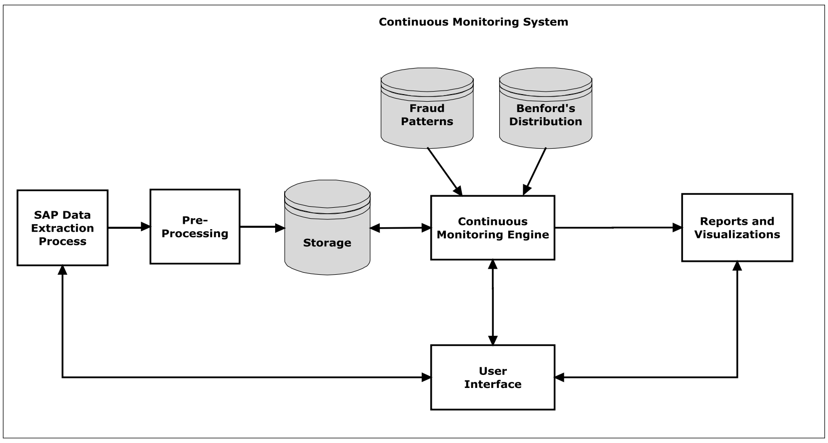

Continuous Monitoring System
Fraud Patterns
Benford's Distribution
SAP Data Extraction Process
Pre-Processing
Storage
Continuous Monitoring Engine
Reports and Visualizations
User Interface

Figure 2. Continuous Monitoring Prototype System

Data required for this process are obtained from SAP tables BKPF (Accounting Document Headers) and BSEG (Accounting Document Line Items). The following fields are extracted from their respective tables for analysis:

Table 2. SAP tables and fields

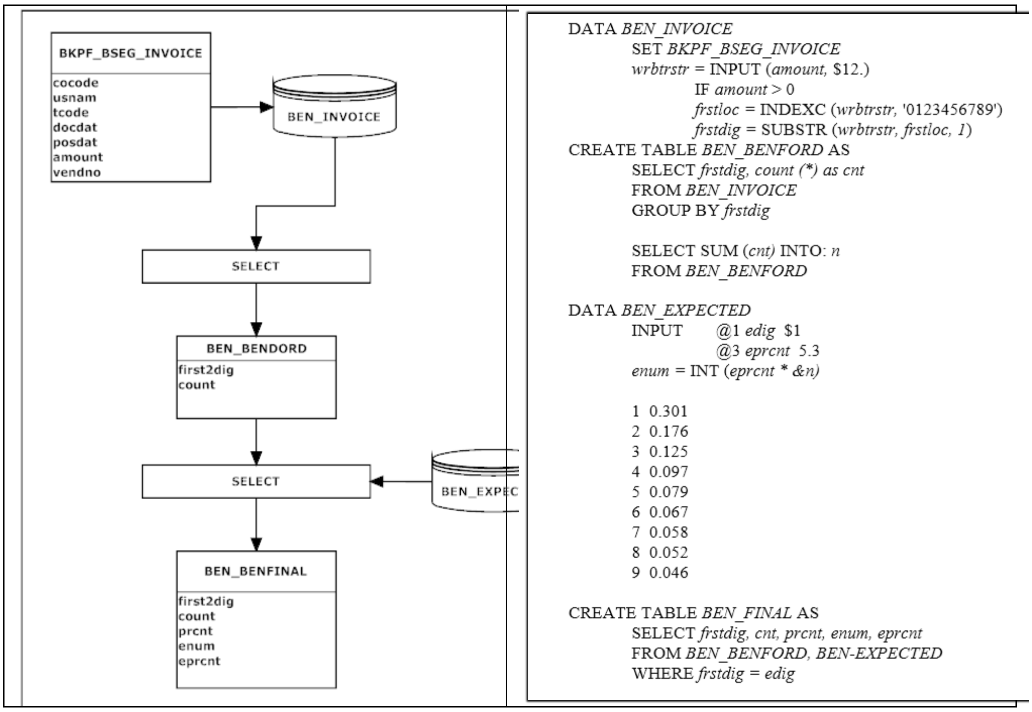
BKPF	BSEG
cocode – company code	amount – invoice amount
tcode – transaction code	vendno – vendor number
posdat – posting date	
usnam – user name	
docdat – document date	
doctype – document type	

Invoice data are extracted from SAP tables BKPF and BSEF. Transactions are pre-processed to extract invoices using the document type field (BLART), DR represent invoices and DZ represent payments. Once invoices are extracted, the analytics process uses SQL (Structured Query Language) code to scan the transaction data (BEN_INVOICE) and extract the first two digits (Figure 3). These digits are stored in a new table (BEN_BENFORD) where they are compared to Benford's expected digit frequencies (BEN_EXPECTED). A counter variable (cnt) sums the number of occurrences of each digit. The resulting data is stored in a new table (BEN_BENFINAL). This table contains information about the digits (firstdig), frequencies (cnt), and percentage (eprcnt). This data is subsequently passed to a procedure that draws the final output (Figures 4 and 6). A similar procedure is performed for payments.

The resultant output is a combination of reports and visualizations. Transaction activities are summarized using bar charts. This presentation method augments the standard text-based reports and support a reduction in information presented to an auditor. Anomalies appear as deviations or spikes from the expected frequencies. These spikes may be indicative of fraud or anomalies that require further investigation by compliance personnel. In order to distinguish between genuine anomalies and procedural anomalies, compliance personnel need to establish what level of deviation from Benford's expected frequencies are the norm in their organization. For example, an organization may be billed regularly for a particular service at the same price. This may yield a procedural anomaly. A second organization may have a similar sequence of invoices and this may due to fraudulent invoices. This is an accounting anomaly. Once a baseline has been established compliance personnel may use this information to filter anomalies occurring for a selected group of vendors.

4.2.1 Data collection

Data was obtained from the SAP ERP systems of two large organizations. Organization 1, a government department, provided a one month sample of accounting transaction data. Organization 2, a global manufacturing company, provided a six month sample of their transaction data. Data from both sites was processed and analyzed. Minimal data cleansing was performed to preformat date and numeric data fields.



```
DATA BEN_INVOICE
        SET BKPF_BSEG_INVOICE
        wrbtrstr = INPUT (amount, $12.)
                IF amount > 0
                frstloc = INDEXC (wrbtrstr, '0123456789')
                frstdig = SUBSTR (wrbtrstr, frstloc, 1)
CREATE TABLE BEN_BENFORD AS
        SELECT frstdig, count (*) as cnt
        FROM BEN_INVOICE
        GROUP BY frstdig

        SELECT SUM (cnt) INTO: n
        FROM BEN_BENFORD

DATA BEN_EXPECTED
        INPUT      @1 edig  $1
                   @3 eprcnt  5.3
        enum = INT (eprcnt * &n)

        1  0.301
        2  0.176
        3  0.125
        4  0.097
        5  0.079
        6  0.067
        7  0.058
        8  0.052
        9  0.046

CREATE TABLE BEN_FINAL AS
        SELECT frstdig, cnt, prcnt, enum, eprcnt
        FROM BEN_BENFORD, BEN-EXPECTED
        WHERE frstdig = edig
```

Figure 3. Process to Detect Benford's Law Anomalies

4.3 Prototype Development

Prototyping involves the creation of a tangible mockup or “proof-of-concept”. The process is non-linear and may be iterative. During the analysis phase, the concept was presented to the case-study organization. Feedback obtained from this process motivated the development of a mock-up. The mock-up was developed into a functional prototype, with the primary objective being to demonstrate viability.

The objective of the prototype is to supplement the knowledge and decision making ability of a human expert. It contains a database of related knowledge and a set of computational rules used to formulate decisions. Quality and effective decision making requires that the embedded knowledge be verified by experts to eliminate consistency and completeness problems (Cojocariu *et al.*, 2005, Singh 2012). Both the computational rules and knowledge base are verified by conducting manual experiments and running the same tests using the prototype to evaluate consistency. These tests evaluated the data input, knowledge base, decision strategies and results.

The knowledge base may be logically correct without being valid. Validation measures how well the prototype conforms to what is being modelled. Measures include productivity measures – to evaluate impact on decisions, process measures – to evaluate impact on decision making, perception measures – to evaluate impact on decision makers; and product measures – to evaluate technical merits of the prototype (Cojocariu *et al.*, 2005). Validation was achieved by demonstrations, hands-on experience and feedback obtained from a series of expert internal auditors (Singh, 2012).

4.4 Verification and validation

Verification and validation are processes to check that software systems meet specifications and that they fulfill their intended purpose. It is a disciplined approach to assessing software products that strives to ensure that quality is built into the software and that it satisfies user requirements (Wallace *et al.*, 1996; IEEE, 2004).

The test data involving simulated transaction activity over a period of one month was randomly generated. A series of 'manual' experiments were then performed using Microsoft Excel to establish control values. These tests were subsequently performed using the prototype. The results produced were reconciled with the control values. The tests served to assess whether the software performed correctly, and that it met the specifications imposed in the design framework. Inconsistencies in results were used to correct errors in the prototypes computational rules and knowledge base.

Validation was achieved by obtaining independent reviews from an expert and a panel of auditing practitioners. The Executive Director of Information Systems Audit of a top international accounting firm reviewed the software. He conducted internal audit tests using his firm's data *(results withheld due to confidentiality*). He indicated that *"... a project of this nature is considered to be of high importance to organizations. It provides a mechanism to pro-actively monitor fraud risk, a key risk in any organization. It also demonstrates a commitment to compliance with Corporate Governance Principles and Recommendations as outlined by ASX Corporate Governance Council."* His commented that automated vendor fraud detection software may provide internal auditors with an approach to efficiently assess the presence of vendor fraud within an organization. A tool of this nature can ensure that the management of the risk of fraud can be undertaken on a more regular or continual basis. He found the prototype to be useful and that graphs and visualizations clearly communicated a message for the user. He also found that the speed of running the tests were *"impressive"*.

Feedback was also from an expert panel of auditing practitioners. In total, 20 members constituted the expert panel. A short presentation and demonstration was made to panel members. Members were provided an opportunity for a hands-on session using the prototype. Their feedback was sought using a survey using a 1 to 7 Likert scale with 1 being 'Strongly disagree' and 7 being 'Strongly agree'. Results are summarized below (Table 3).

Table 3. Feedback from Expert Panel

#	Aspect	Mean	Variance	Std. Dev.
1	**Operation**			
1.1	Easy to use	5.87	0.45	0.81
1.2	User-friendly	5.78	0.45	0.67
2	**Reports & Visualizations**			
2.1	Useful in aggregating an enormous amount of information	6.09	0.54	0.73
2.2	Enables effective exploration of data in a graphical format	6.13	0.57	0.76
2.3	Enables easy identification of relationships or patterns in data	6.17	0.60	0.78
2.4	Enhances investigation and analysis for potential fraud	6.22	0.54	0.74
2.5	Are an important tool in a fraud investigators toolkit	6.04	0.77	0.88
3	**Performance**			
3.1	Generates results much faster than doing a similar task manually	6.35	0.43	0.65
3.2	Potential to save costs due to improved fraud detection	6.13	0.39	0.63
3.3	Potential to reduce future fraud by early detection	6.22	0.45	0.67
3.4	May reduce time taken to identify potential fraud in an organization	6.30	0.49	0.70

They found the visualizations were easy to understand, were useful in aggregating large volumes of data and enabled easy identification of anomalies in accounts payable transactions. They also found the prototype to be an improvement over basic analytical tools. Results are discussed in the following section.

5. Findings and discussion

SAS No. 56 requires auditors to use analytical procedures in planning the nature, timing and extent of auditing procedures (AICPA, 1988). In this study we apply data analytics to identify anomalies in accounting transactions. The analysis focuses on digit and number patterns, and is based on a mathematical phenomenon known as Benford's Law (Benford, 1938). The tests relate to the first-two digits. The analysis is suited to cases where transactions are stored in an electronic format. Auditors often encounter large data sets, and consequently an audit of even a small percentage of these transactions is impractical and economically infeasible. The Auditing Standards Board's SAS No. 82, titled "Consideration of Fraud in a Financial Statement Audit", states that there is a responsibility on the part of auditors to detect material fraud. The statement calls for specific and ongoing assessment of the potential for material misstatement caused by fraud. Use of data analytics may fulfill some of the auditor's obligations related to fraud and anomaly detection. Given the decline in cost and the increase in processing speed of computers, the use of analytical procedures has become economically feasible.

Most accounting datasets conform to Benford's distribution, and are appropriate candidates for digital analysis (Hill, 1995). These accounts consist of transactions that result from combining numbers, for example, accounts receivable is the number of items purchased multiplied by the price per item. Similarly, accounts payable and most revenue and expense accounts are expected to conform. In general, results from Benford's analysis are more reliable if the entire account population is analyzed rather than sampling the account. This is because the larger the number of transactions in the data set, the more accurate the analysis (Durtschi *et al.*, 2004)

In this study, Benford's analysis was performed on the accounts payable transactions of the case organizations, in particular, their invoice and payment amounts, because these transactions satisfy the following conditions (Nigrini, 2012):

- all the numbers are recorded in the same unit of measurement;
- the numbers do not have an arbitrary maximum and/or minimum cut-off point;
- the numbers are not assigned, such as personal identification numbers, invoice numbers and postal codes;
- the numbers are not influenced by human thought, such as psychological supermarket prices (which often have 9 as a last digit, for example $5.99).

5.1 Case study 1 – A Government Department

A detailed analysis of invoice and payment transactions was performed by the prototype software and is presented below.

***User profiles* -** a total of 5,996 invoices and 3,135 payments were recorded during the analysis period. There were 81 active system users. Of these 81 users, 69 performed accounts payable activities (Table 4).

Table 4. Activities performed by users (Case 1)

# Transactions	Description of Activity	# Users
5,996	posting document (FB01)	64
3,094	parameters for automatic payment (F110)	2
41	post outgoing payments (FBZ2)	3

(Note: In Table 3, SAP T-code FB01 is a generic posting transaction. To ensure only invoices and payments are analyzed, all transactions are pre-filtered using the document type field (BLART), DR – invoices and DZ – payments from table BKPF.)

***Transaction analysis* -** accounts payable transactions were analyzed and the findings are summarized below (Table 5). In total 5,996 invoices were entered for a total dollar value of $10,045,281.90; and 3,136 payments were processed for a total dollar value of $13,226,457.57.

Table 5. Summary of accounts payable transactions (Case 1)

Activity	Value
number of invoices entered	5,996
number payments processed	3,135
total value of invoices entered	$ 10,045,281.90
total value of payments processed	$ 13,226,457.57
top vendor by invoice	0001001516
total value of invoices for this vendor	$ 1,472,887.36
top vendor by payment	0001001516
total value of payments for this vendor	$ 1,472,887.36

Analysis of the first two digits for vendor invoices revealed spikes at **10**, **12**, **19**, **24** and **49** (Figure 4). Spikes also occurred at **10**, **11**, **12**, **14**, **18**, **19** and **22** for vendor payments (Figure 4, the underlying data is shown in Figure 5). The largest of these spikes was 49 for invoices and 22 for payments. This information was flagged by internal audit for further investigation. *(Further details of this investigation were not provided by the organization).*

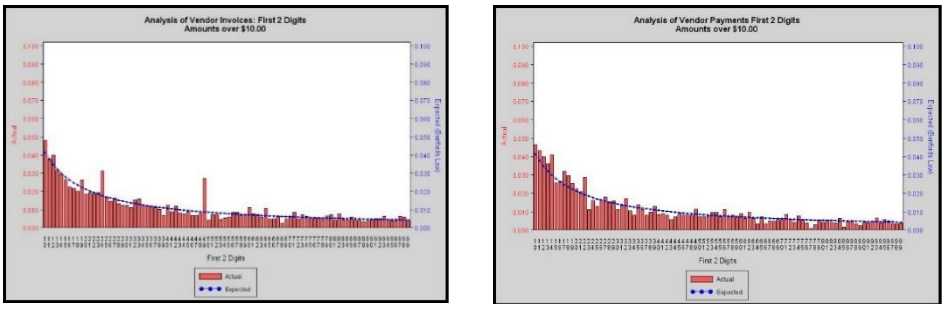
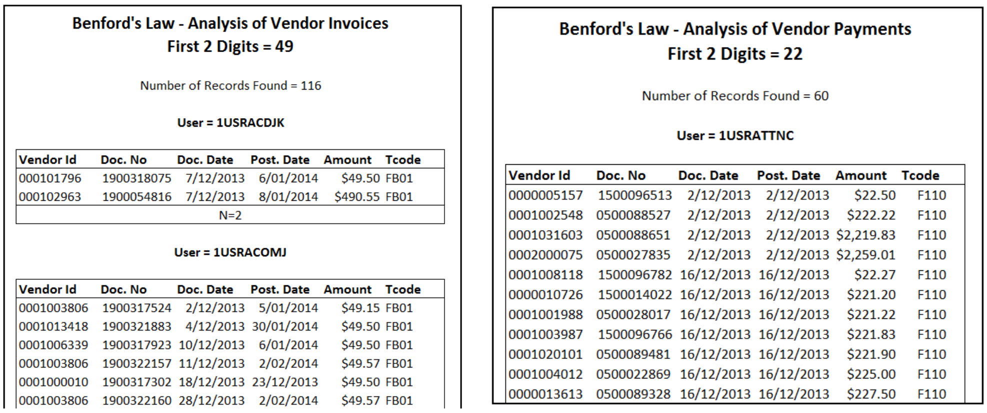


Figure 4. Visual Results – Invoice and Payment Transactions (Case 1)



Benford's Law - Analysis of Vendor Invoices

First 2 Digits = 49

Number of Records Found = 116

User = 1USRACDJK

Vendor Id	Doc. No	Doc. Date	Post. Date	Amount	Tcode
000101796	1900318075	7/12/2013	6/01/2014	$49.50	FB01
000102963	1900054816	7/12/2013	8/01/2014	$490.55	FB01
N=2					

User = 1USRACOMJ

Vendor Id	Doc. No	Doc. Date	Post. Date	Amount	Tcode
0001003806	1900317524	2/12/2013	5/01/2014	$49.15	FB01
0001013418	1900321883	4/12/2013	30/01/2014	$49.50	FB01
0001006339	1900317923	10/12/2013	6/01/2014	$49.50	FB01
0001003806	1900322157	11/12/2013	2/02/2014	$49.57	FB01
0001000010	1900317302	18/12/2013	23/12/2013	$49.50	FB01
0001003806	1900322160	28/12/2013	2/02/2014	$49.57	FB01

Benford's Law - Analysis of Vendor Payments

First 2 Digits = 22

Number of Records Found = 60

User = 1USRATTNC

Vendor Id	Doc. No	Doc. Date	Post. Date	Amount	Tcode
0000005157	1500096513	2/12/2013	2/12/2013	$22.50	F110
0001002548	0500088527	2/12/2013	2/12/2013	$222.22	F110
0001031603	0500088651	2/12/2013	2/12/2013	$2,219.83	F110
0002000075	0500027835	2/12/2013	2/12/2013	$2,259.01	F110
0001008118	1500096782	16/12/2013	16/12/2013	$22.27	F110
0000010726	1500014022	16/12/2013	16/12/2013	$221.20	F110
0001001988	0500028017	16/12/2013	16/12/2013	$221.22	F110
0001003987	1500096766	16/12/2013	16/12/2013	$221.83	F110
0001020101	0500089481	16/12/2013	16/12/2013	$221.90	F110
0001004012	0500022869	16/12/2013	16/12/2013	$225.00	F110
0000013613	0500089328	16/12/2013	16/12/2013	$227.50	F110

Figure 5. Underlying Data – Invoice and Payment Transactions (Case 1)

5.2 Case study 2 – A Global Manufacturing Company

User profiles - A total of 45,368 invoice and 8,862 payment activities were recorded during the analysis period (Table 6). There were 58 active system users (note: sum of users in the table below may add up to more than 81 as some users may have performed more than one type of activity). They performed the following activities (Table 7).

Table 6. Activities performed by users (Case 2)

# Transactions	Description of Activity	# Users
24,690	invoice entry (FB60)	42
20,678	posting document (FB01)	26
8,343	parameters for automatic payment (F110)	24
459	post outgoing payments (FBZ2)	7
60	payment with printout (FBZ4)	5

Transaction analysis - accounts payable transactions were analyzed and the findings are summarized below (Table 4). In total 45,368 invoices were entered for a total dollar value of $186,449,162.56; and 8.862 payments were processed for a total dollar value of $28,106,039.65.

Table 7. Summary of accounts payable transactions (Case 2)

Activity	Value
number of invoices entered	45,368
number payments processed	8,862
total value of invoices entered	$186,449,162.56
total value of payments processed	$28,106,039.65
top vendor by invoice	0000030044
total value of invoices for this vendor	$114,660,580.29
top vendor by payment	0000100027
total value of payments for this vendor	$2,933,273.73

Analysis of the first two digits for vendor invoices revealed spikes at **11**, **22**, **27**, **36**, **45**, **54** and **67**. Spikes also occurred at **22**, **27**, **36**, **37** and **45** for vendor payments (Figure 6, the underlying data is shown in Figure 7). Other smaller spikes were also observed for invoices and payments. The largest of these spikes was 36 for invoices and 22 for payments. Spike **36** was selected as this was the largest spike**.** The subsequent report contained 1217 records, of all invoice amounts containing **36** as the first two digits. Several **identical** amounts appeared to have been recorded for the **same vendors**. These transactions were entered by different users. A follow up investigation was conducted and several duplicate invoices were discovered. On conclusion of the investigation this organization implemented wide-spread changes to their policies. Further investigations were conducted based on the red flags raised by the investigation. The findings also revealed the potential vulnerability to vendor fraud that the organization faced due to poor internal controls. *(Further details of this investigation were not provided by the organization).*

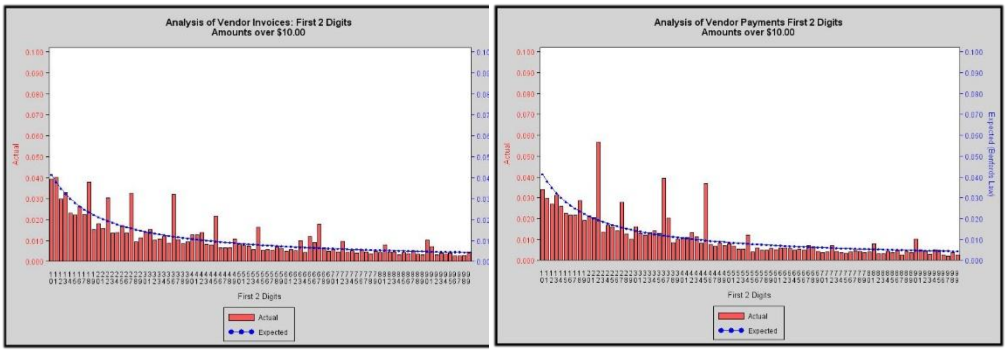
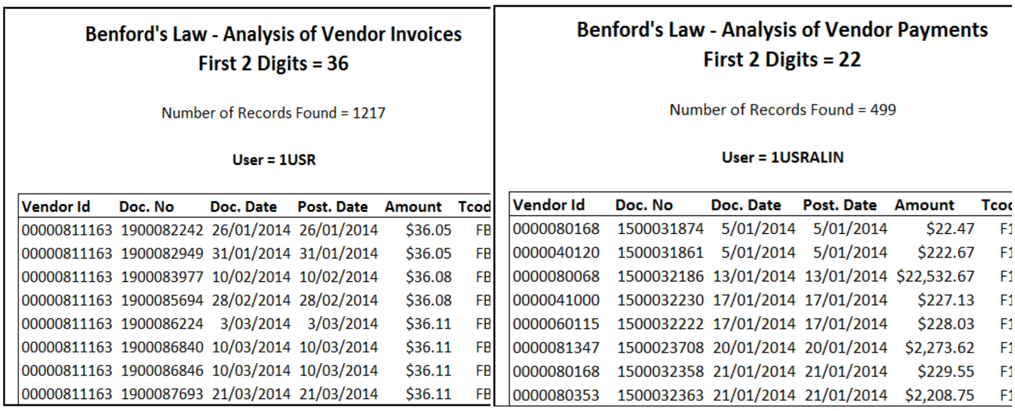


Figure 6. Visual Results – Invoice and Payment Transactions (Case 2)



Benford's Law - Analysis of Vendor Invoices
First 2 Digits = 36

Number of Records Found = 1217

User = 1USR

Vendor Id	Doc. No	Doc. Date	Post. Date	Amount	Tcod
00000811163	1900082242	26/01/2014	26/01/2014	$36.05	FB
00000811163	1900082949	31/01/2014	31/01/2014	$36.05	FB
00000811163	1900083977	10/02/2014	10/02/2014	$36.08	FB
00000811163	1900085694	28/02/2014	28/02/2014	$36.08	FB
00000811163	1900086224	3/03/2014	3/03/2014	$36.11	FB
00000811163	1900086840	10/03/2014	10/03/2014	$36.11	FB
00000811163	1900086846	10/03/2014	10/03/2014	$36.11	FB
00000811163	1900087693	21/03/2014	21/03/2014	$36.11	FB

Benford's Law - Analysis of Vendor Payments
First 2 Digits = 22

Number of Records Found = 499

User = 1USRALIN

Vendor Id	Doc. No	Doc. Date	Post. Date	Amount	Tcoc
0000080168	1500031874	5/01/2014	5/01/2014	$22.47	F1
0000040120	1500031861	5/01/2014	5/01/2014	$222.67	F1
0000080068	1500032186	13/01/2014	13/01/2014	$22,532.67	F1
0000041000	1500032230	17/01/2014	17/01/2014	$227.13	F1
0000060115	1500032222	17/01/2014	17/01/2014	$228.03	F1
0000081347	1500023708	20/01/2014	20/01/2014	$2,273.62	F1
0000080168	1500032358	21/01/2014	21/01/2014	$229.55	F1
0000080353	1500032363	21/01/2014	21/01/2014	$2,208.75	F1

Figure 7. Underlying Data – Invoice and Payment Transactions (Case 2)

When selecting Benford's analysis as an approach to detect anomalies it is important to consider which types of accounts may be used effectively. Some populations of accounting data may not conform to Benford's distribution. For example, assigned numbers, such as check numbers, purchase order numbers, numbers such as product or service prices, or ATM withdrawals, do not follow Benford's law (Nigrini & Mittermaier, 1997). Assigned numbers follow a uniform distribution rather than Benford's distribution. Prices are often set to fall below psychological barriers, for example $1.99 is perceived as much lower than $2.00, thus prices tend to cluster below psychological barriers. ATM withdrawals are often in pre-assigned even amounts.

The value of Benford's law lies in its ability to identify accounts likely to have fraud. Using the entire dataset reduces the effects of random sampling that auditors usually use when employing traditional audit methods. However, data analytics is not a 'silver bullet' in detecting fraud. Firstly the accuracy of the analysis when using actual data may be questionable. Secondly, the probability of fraud existing in the data is unknown. To accurately determine the effectiveness of Benford's law requires auditors to compare accounts containing actual fraud with accounts that do not. However, sourcing such data may be difficult as most companies are not willing to disclose their accounts regardless of whether fraud is present or not.

The data-set chosen ought to conform Benford's distribution. Since accounting-related data can be expected to conform, it is a suitable candidate (Hill, 1995). The size of the data set also matters. Results will be more accurate if the entire population is used instead of a small sample. When considering the usefulness of the results produced, consideration must be given to the outcomes produced by the analysis. As the test compares the actual number of occurrences to an expected proportion, some deviation will occur naturally, namely, an exact fit cannot be expected. Auditors will need to make a decision as to what level of deviation is significant. Failing to consider this characteristic may result in too many false positives. Furthermore, other types of frauds/anomalies exist that are unable to be detected using this approach. Therefore, Benford’s analysis should be used to complement other detection strategies.

A key contribution of the study is the development of prototype software to automate extraction and analysis to accounting transactions. This enables the entire population of transactions for a specified time period to be analyzed. This approach is in contrast with the traditional or manual audit approach which is limited because it reviews only a small percentage of a large population of transactions. Furthermore as the demand for continuous auditing and monitoring increases, the innovative techniques developed in this study can certainly be adopted in practice. This will provide compliance personnel with a degree of assurance shortly after transactions are processed, rather than having to wait for the annual audit.

6. Limitations and conclusion

Fraud is a global problem that continues to grow annually. Results from the ACFE (2016b) Report to the Nation on Occupational Fraud and Abuse highlights the significance and pervasiveness of the fraud problem. The Report concluded that the projected annual loss due to fraud is approximately $3.7 trillion worldwide. Furthermore an AuditNet survey (2012) of more than 1500 auditors concluded that the use of data analytics tools and techniques are not being maximized in routine audit activities. Therefore the financial impact of fraud appears to be increasing yet resources and technology are not being effectively deployed to address the problem.

Enhancing the ability of organizations to identify ‘red flags’ of potential fraud may have a positive impact on the economy. An effective model that facilitates proactive detection may potentially save costs and reduce the propensity of future fraud by early detection of suspicious user activities. Enterprise systems generate hundreds of thousands to millions of transactions annually. This enormous amount of transactions makes it difficult to find few potentially anomalous instances among legitimate transactions. Without the availability of proactive tools that continuously monitor transactions, identifying and investigating suspicious activities becomes overwhelming.

A limitation is that Benford’s analysis identifies fraudulent transactions based on whether digits appear in an expected proportion. A significant deviation from expectations occurs when a person perpetrating a fraud has either added observations or has removed observations which results is a data-set that does not conform to Benford’s distribution. Each action would result in an observable deviation from expectations, provided the number relative to the sample is large enough for statistical detection. Therefore, when a fraud occurs in which transactions are never recorded (for example, off-the-books fraud), as in the case of bribes, kickbacks or asset thefts, digital analysis cannot be expected to detect the absence of transactions.

A further limitation of the prototype is the possibility of Type I errors. A Type I error, also known as a false positive, occurs when a test rejects a true null hypothesis or general position (Shuttleworth, 2008). For example, if the null hypothesis states that round dollar invoices are a symptom of fraud, and round dollar invoices do indeed exist, but the prototype rejects this hypothesis, it may falsely ignore potentially fraudulent transactions. It is essential to recognize that the prototype is intended to assist an auditor by facilitating early detection of potentially fraudulent activities. The digits approach, whilst increasing the chances of Type I errors, also increases the chances of finding fraudulent activities (Cleary and Thibodeau, 2005). The onus is on the auditor be aware of such situations and to conduct further tests to reduce such errors.

A key goal and contribution of this paper was to demonstrate the feasibility of implementing Benford's analysis in continuous monitoring applications by exploiting audit trails in enterprise systems. The concept was demonstrated by designing prototype software. Accounting audit trails are routinely extracted from a SAP enterprise system, pre-processed, and analyzed (Figure 2). The prototype demonstrates how this strategy can be implemented, though it is only a 'proof of concept' tool, not a commercial application for use by auditors and other end-users.

We conclude that Benford's analysis, when used correctly, is a useful tool for identifying suspicious transactions for further analysis. Because of its usefulness, Benford's law may identify possible errors, potential fraud or other irregularities in transaction data. The analysis is particularly useful because it does not use aggregated data, rather it may be applied all available data. Consequently, it may highlight specific transactions and/or activities that require further investigation. While Benford's analysis has several advantages, the following limitations are highlighted; (i) due care must be exercised in interpreting the results of the analysis, (ii) this method is only appropriate for data sets that conform to the Benford distribution, and (iii) this is not a 'silver bullet' to detecting frauds, and ought to be used to complement other analytics techniques.

References

ACFE (2016a) *Fraud Examiners Manual,* International Edition.

ACFE (2016b) "Report to the Nation on Occupational Fraud and Abuse", http://www.acfe.com/rttn.aspx. *Accessed:* 10/05/2016

AICPA (1988) Analytical Procedures (AU Section 329). Statement on Auditing Standards No. 56. New York, NY:American Institute of Certified Public Accountants.

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*, vol. 7 (2): 137-161

Alles, M. G., Kogan, A. & Vasarhelyi, M. A. (2002) "Feasibility and Economics of Continuous Assurance", *AUDITING: A Journal of Practice & Theory*, vol. 21 (1): 125-138

Asur, S. & Hufnagel, S. (1993) Taxonomy of rapid-prototyping methods and tools. *IN Proceedings Rapid System Prototyping, 1993. Shortening the Path from Specification to Prototype. Proceedings, Fourth International Workshop on Rapid Prototyping*, 42-56

AuditNet (2012) "AuditNet 2012 State of Technology Use by Auditors", *AuditNet LLC*, http://www.auditnet.org/. *Accessed:* 27/02/2013

Benford, F. (1938) "The Law of Anomalous Numbers", *Proceedings of the American Philosophical Society*, vol. 78 (4): 551-572.

Berton, L. (1995) "He’s got their number: scholar uses math to foil financial fraud", *Wall Street Journal*, 10**,** B1.

Best, P. J. (2000) “SAP R/3 Audit Trail Analysis”, *IN Proceedings Sapphire 2000. 4th Annual SAP Asia Pacific Institute of Higher Learning Forum*

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*, vol. 4 (1): 39-60

Brown, C. E., Wong, J. A. & Baldwin, A. A. (2007) "A Review and Analysis of the Existing Research Streams in Continuous Auditing", *Journal of Emerging Technologies in Accounting*, vol. 4: 1-28.

Budde, R. & Zullighoven, H. (1990) “Prototyping revisited”, *IN Proceedings CompEuro '90. Proceedings of the 1990 IEEE International Conference on Computer Systems and Software Engineering*, pp. 418-427

Camerer, C. (2003) *Behavioral game theory: experiments in strategic interaction*, Russell Sage Foundation, London.

Carslaw, C. A. (1988) "Anomalies in income numbers: Evidence of goal oriented behavior", *Accounting Review*, vol. 63: 321-327

Christian, C. W. & Gupta, S. (1993) "New evidence on secondary evasion", *The Journal of the American Taxation Association*, vol. 15 (1): 72-87

Ciaponi, F. & Mandanici, F. (2015) "Using Digital Frequencies to Detect Anomalies in Receivables and Payables: An Analysis of the Italian Universities", *Journal of Economic and Social Development*, vol. 2 (1): 86-108

Cleary, R. & Thibodeau, J. C. (2005) "Applying digital analysis using Benford's law to detect fraud: the dangers of type I errors", *Auditing: A Journal of Practice & Theory*, vol. 24 (1): 77-81.

Coderre, D. G. (2005) *Global Technology Audit Guide. Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, IN IIA (Ed.). Florida, IIA.

Cojocariu, A., Munteanu, A. & Sofran, O. (2005) "Verification, Validation and Evaluation of Expert Systems in Order to Develop a Safe Support in the Process of Decision Making", *Computational Economics, EconWPA,* http://ideas.repec.org/p/wpa/wuwpco/0510002.html. *Accessed:* 10/11/2011

Da Silva, C. G. & Carreira, P. M. (2012) "Selecting audit samples using Benford's Law", *Auditing: A Journal of Practice & Theory*, vol. 32 (2): 53-65.

De Marchi, S. & Hamilton, J. T. (2006) "Assessing the accuracy of self-reported data: an evaluation of the toxics release inventory", *Journal of Risk and uncertainty*, vol. 32 (1): 57-76

Debreceny, R. S. & Gray, G. L. (2010) "Data mining journal entries for fraud detection: An exploratory study", *International Journal of Accounting Information Systems*, vol. 11 (3): 157-181

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*, vol. 19 (2): 7-27.

Durtschi, C., Hillison, W. & Pacini, C. (2004) "The effective use of Benford's law to assist in detecting fraud in accounting data", *Journal of Forensic Accounting*, vol. 5 (1): 17-34.

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004) "Design Science in Information Systems Research", *MIS Quarterly*, vol. 28 (1): 75-105.

Hill, T. P. (1988) "Random-number guessing and the first digit phenomenon", *Psychological Reports*, vol. 62 (3): 967-971.

Hill, T. P. (1995) "A statistical derivation of the significant-digit law", *Statistical Science***,** vol. 10 (4): 354-363.

Hogan, C. E., Rezaee, Z., Riley Jr, R. A. & Velury, U. K. (2008) "Financial statement fraud: Insights from the academic literature", *Auditing: A Journal of Practice & Theory*, vol. 27 (2): 231-252.

IEEE (2004) "Guide to the Software Engineering Body of Knowledge (SWEBOK)", *IEEE Computer Society*, http://www.computer.org/portal /web/swebok/html/ch11. Accessed: 14/11/2011

Kim, Y., Hsu, J. & Stern, M. (2006) "An update on the IS/IT skills gap", *Journal of Information Systems Education*, vol. 17 (4): 395-402.

Kogan, A., Sudit, E. F. & Vasarhelyi, M. A. (1999) "Continuous online auditing: A program of research", *Journal of Information Systems*, vol. 13 (2):87-103.

Kotb, A. & Roberts, C. (2011) "The Impact of E-Business on the Audit Process: An Investigation of the Factors Leading to Change", *International Journal of Auditing*, vol. 15 (2): 150-175.

Kuhn Jr, J. R. & Sutton, S. G. (2010) "Continuous Auditing in ERP System Environments: The Current State and Future Directions", *Journal of Information Systems,*vol. 24 (1): 91-112.

Lanza, R. B. (2003) *Proactively Detecting Occupational Fraud Using Computer Audit Reports*, Florida, The IIA Research Foundation.

Messier Jr, W. F., Simon, C. A. & Smith, J. L. (2012) "Two decades of behavioral research on analytical procedures: What have we learned?", *Auditing: A Journal of Practice & Theory,* vol. 32 (1): 139-181

Newcomb, S. (1881) "Note on the Frequency of Use of the Different Digits in Natural Numbers", *American Journal of Mathematics,* vol. 4 (1): 39-40.

Nigrini, M. (1994) "Using digital frequencies to detect fraud", *The White Paper*, vol. 8 (2):3-6.

Nigrini, M. (2012) *Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection*, John Wiley & Sons.

Nigrini, M. J. (1996) "A taxpayer compliance application of Benford's law", *The Journal of the American Taxation Association*, vol. 18 (1): 72-91.

Nigrini, M. J. (1999) "I've got your number", *Journal of Accountancy*, vol. 187 (5): 79-83.

Nigrini, M. J. & Miller, S. J. (2009) "Data diagnostics using Second-Order Tests of Benford's law", *Auditing: A Journal of Practice & Theory*, vol. 28 (2): 305-324.

Nigrini, M. J. & Mittermaier, L. J. (1997) "The use of Benford's Law as an Aid in Analytical Procedures", *Auditing*, vol. 16 (2):52-67.

Rezaee, Z., Sharbatoghlie, A., Elam, R. & McMickle, P. L. (2002) "Continuous Auditing: Building Automated Auditing Capability", *Auditing*, vol. 21 (1): 147-163.

Schraepler, J. P. & Wagner, G. G. (2005) "Characteristics and impact of faked interviews in surveys–An analysis of genuine fakes in the raw data of SOEP", *Allgemeines Statistisches Archiv*, vol. 89 (1): 7-20.

Shuttleworth, M. (2008) "Experimental Errors: Type I Error and Type 2 Error", *Experiment-Resources.com,* http://www.experiment-resources.com/type-I-error.html. Accessed: 16/06/2011

Singh, K. (2012) "A Conceptual Model for Proactive Detection of Potential in Enterprise Systems: Exploiting SAP Audit Trails to Detect Asset Misappropriation". *Department of Accounting, Economics and Finance,* University of Southern Queensland, PhD Thesis.

Singh, K. H., Best, P. J., Bojilov, M. & Blunt, C. (2014) "Continuous Auditing and Continuous Monitoring in ERP Environments: Case Studies of Application Implementations", *Journal of Information Systems*, vol. 28 (1): 287-310.

Singleton, T. W. & Singleton, A. J. (2007) "Why don't we detect more fraud?", *Journal of Corporate Accounting & Finance,* vol. 18 (4): 7-10.

Slijepcevic, S. & Blaskovic, B. (2014) "Statistical detection of fraud in the reporting of Croatian public companies", *Financial Theory and Practice,* vol. 38 (1): 81.

Tam Cho, W. K. & Gaines, B. J. (2007) "Breaking the (Benford) law: Statistical fraud detection in campaign finance", *The American Statistician*, vol. 61 (3): 218-223

Thomas, J. K. (1989) "Unusual patterns in reported earnings", *Accounting Review*, 64 (4): 773-787

Trompeter, G. & Wright, A. (2010) "The World Has Changed - Have Analytical Procedure Practices?", *Contemporary Accounting Research*, vol. 27 (2): 669-700

Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S. & Littley, J. (2012) "The acceptance and adoption of continuous auditing by internal auditors: A micro analysis", *International Journal of Accounting Information Systems*, vol. 13 (3): 267-281

Vasarhelyi, M. A., Alles, M. & Williams, K. T. (2010) Continuous Assurance for the Now Economy. *A Thought Leadership Paper for the Institute of Chartered Accountants in Australia.*

Wallace, D. R., Ippolito, L. M. & Cuthill, B. (1996) "NIST Special Publication 500-234. Reference Information for the Software Verification and Validation Process", http://hissa.nist.gov/HHRFdata/Artifacts/ITLdoc/234/val-proc. html. Accessed: 14/11/2011

Zheng, Y., Glass, R. & Olinsky, A. (2017) "An Application of Benford's Law to Detect Data Misrepresentation in Mutual Fund Reporting", *Academy of Business Research Journal*, vol. 1:65-73.