ISSN 2392-1641

Economics and Business Review

Volume 2 (16) Number 4 2016

CONTENTS

Poznań University of Economics and Business Press

Paper based publication

ISSN 2392-1641

POZNAŃ UNIVERSITY OF ECONOMICS AND BUSINESS PRESS
ul. Powstańców Wielkopolskich 16, 61-895 Poznań, Poland
phone +48 61 854 31 54, +48 61 854 31 55, fax +48 61 854 31 59
www.wydawnictwo-ue.pl, e-mail: wydawnictwo@ue.poznan.pl
postal address: al. Niepodległości 10, 61-875 Poznań, Poland

Printed and bound in Poland by:
Poznań University of Economics and Business Print Shop

Circulation: 230 copies

Economics and Business Review

Volume 2 (16) Number 4 2016

CONTENTS

ARTICLES

MISCELLANEA

BOOK REVIEWS

Economics and Business Review, Vol. 2 (16), No. 4, 2016: 45–64
DOI: 10.18559/ebr.2016.4.3

Accounting frauds – review of advanced technologies to detect and prevent frauds[1]

Shay Y. Segal[2]

Abstract: In past decades, accounting fraud has adversely affected economies worldwide. Therefore, effective measures and methods ought to be employed in order to efficiently prevent and detect accounting fraud in a rapidly changing and technology-based business environment. Data mining methods can assist in prevention and detection of fraudulent transactions as it enables the use of past cases of fraud to build models that can recognize and spot the risk of fraud and can design new techniques for preventing fraudulent financial reporting. This article reviews the concept of accounting fraud, and focuses on some of the available data mining tools and methodologies , as well as other commuter-based techniques and tools that are available to order to assist in preventing accounting fraud and detecting if fraudulent acts have been committed. The article asserts the importance of using the available computer-based and data mining techniques as a prevention mechanism by detecting financial statement fraud, concluding that data mining software propose a good supporting procedure which offers an effective solution to the problem of detecting fraudulent transactions and accounting frauds.

Keywords: accounting frauds, preventing frauds, advanced technologies, ERP, XBRL.

JEL codes: JEL M40.

Introduction

As new data mining techniques and tools were presented in the last decades, the research of the applicability of data mining techniques for financial accounting fraud detection of is a promising field. This paper presents a review of the possibilities of application of data mining techniques to detect and prevent financial accounting fraud. The paper focuses on an approach that attempts to detect and prevent frauds in accounting, by addressing the shortcomings in

[1] Article received 18.04.2016 accepted 2 November 2016.

[2] Jerusalem College of Technology, the Management and Accounting Department, Havaad Haleumi 21st., Jerusalem 9372115, Israel, shillat@gmail.com.

previous attempts by auditors and investigators who were trained in accounting and auditing methods.

In the past decade, we have witnessed crises and collapses of large public companies with disastrous implications (for example, AIG, WorldCom, Enron, etc.) as a result of sophisticated fraud and questionable accounting techniques that were used for creating misrepresentation of the company's profits.

According to Chan and Vasarhelyi [2011], traditional auditing paradigm relies on periodic reviews, a reactive approach, manual audit procedures, centered around labor and time intensive audit procedures, testing consists of analytical review and subsequent details testing and sampling, controls testing occurs independently of details testing , and humans perform the testing. In a changing business environment, a different approach may be required.

In the past decades, we have also witnessed an era of sophisticated IT tools, with developments such as Data Mining, ERP (Enterprise Resource Planning software), BI tools, and dedicated software like XBRL (Extensible Business Reporting Language), etc. Many traditional common control mechanisms are no longer applicable. Moreover, the role of an auditor is changing, as a highly-complex ERP system are responsible for electronically sending, receiving, and storing information.

Auditors should be able to monitor these complex ERP systems continuously, in order to identify and prevent frauds. The availability of Big Data in these new ERP systems creates new opportunities for auditors. One of these opportunities resides in several improved methods to detect fraud. Whether it is fraudulent financial reporting or misappropriation of assets, the development of innovative techniques outside the realms of accounting could aid auditors to assess the likelihood and fraud risk.

The aim in this research is to explore the tools, as well as the different ways of utilizing current technology to assist auditors and the auditing environment in improving fraud deterrence and detection. In order to achieve this goal, we will analyze three principal aspects: the current IT environment and the role of auditing in this context; definitions of fraud and threats; approaches to detect frauds.

This paper covers not all the technical solutions to detect and prevent frauds in Accounting as there are a multitude of them. Rather it focuses on an approach that attempts to address the shortcomings in previous attempts by auditors and investigators who are trained in traditional accounting and auditing methods.

The paper is diveded into X sections. The first two Sections describe the essence and nature of fraud in general. Section 3 is devoted to a review of the characteristics of accounting fraud. Section 4 describes the different types of accounting fraud, Section 5 is devoted to classification of data mining techniques and applications for financial accounting fraud detection. Section 3 provides distribution of the research literature as per the applications and techniques of data mining for the detection of financial accounting fraud. Sections 5 and 6 describe the recent changes in the accounting IT environment and the available IT tools. Section 7 summarizes and outlines future directions of fraud prevention.

1. Essence of accounting frauds

Accounting is an activity of service to provide useful information regarding the economic units to the decision makers inside and outside of them. Therefore, accounting must identify and analyze as well as measure and record effectively the activities of the economic units and report effectively to the users interested in this information.

According to Jones [2011], a fair presentation uses the flexibility within accounting to give a true and fair picture of the accounts so that they serve the interests of users. Creative accounting uses the flexibility within accounting to manage the measurement and presentation of the accounts so that they serve the interests of preparers. Impression management occurs when the flexibility of the accounts (especially narrative and graphs) is being used to convey a more favorable view than is warranted of a company's results serving the interests of preparers. According to Jones [2011], the essence of fraud, is Moving outside the Regulatory Structure intentionally to give a false representation of the accounts.

Jones [2011] notes that accounting fraud occurred through history, from ancient times (Mesopotamia), through medieval times (Italy in fourteenth century and England in fifteenth century) and up until our days. Accounting fraud also occurs throughout the globe, as Jones [2011] mentions some accounting schemes that took place in the USA, UK, Australia, Germany, Greece, China, India, Italy, Japan, Netherlands Spain and Sweden.

After reviewing more than 58 cases of accounting fraud, Jones [2011] has found that a common theme to accounting frauds was that they were promulgated by strong personalities with charismatic persuasion powers, The strongest motivation from which fraud arises was managers' personal gain and benefits, and a second motive was covering up bad performance, Fraud was always enabled by failure of internal controls and poor corporate governance, as well as failure of external auditors.

The traditional audit paradigm is outdated in the real time economy. Innovation of the traditional audit process is necessary to support real time assurance. In the real time economy [*The Real* 2002], timely and reliable financial information is critical for day to day business decisions regarding strategic planning, raising capital, credit decisions, and supplier or vendor partnerships.

In the past decade we have seen crises and collapses of large public companies, when the implications were disastrous (for example, Enron, WorldCom, AIG, etc.). These collapses were the result of a complex system of sophisticated fraud and dubious accounting tricks for the purpose of the creation of misrepresentation of tremendous profits [Hake 2005]. Financial reporting frauds and earnings manipulation have attracted high profile attention recently. There have been several cases by businesses of what appears to be financial statement fraud, which have been undetected by the auditors. According to Wells [2005: 325–327], financial statement fraud is harmful in many ways. For example:

- Undermines the reliability, quality, transparency, and integrity of the financial reporting process,
- Jeopardizes the integrity and objectivity of the auditing profession, especially auditors and auditing firms, e.g. Andersen,
- Causes bankruptcy or substantial economic losses by the company engaged in financial statement fraud.

2. What is fraud?

Fraud "relates to wrongful or criminal deception that results in financial or personal gains" [Kabir Usman 2013: 4]. According to the National Fraud Authority [Button 2009], "fraud embraces a broad scope of different crimes," which have been complied into a very comprehensive list of typology, also known as Levi's Typology List of Fraud by Victim Note.

Fraud researchers have found that several elements are present in all fraudulent activities: A perceived pressure; second, a perceived opportunity, and a way to rationalize the fraud as acceptable and consistent with one's personal code of ethics [Albrecht, Albrecht, and Dunn 2006].

Fraud and its subtype, identity theft, are becoming more common with the use of e-commerce, computer-based technologies, and the Internet. Fraud crimes involve now innovative technologies, as an immediate contact with the physical surrounding is no longer necessary in the virtual world [Kunz and Wilson 2004]. As economic wealth and currency are represented by virtual numbers and not real assets, their vulnerability increases, since they can be reached from virtually anywhere. According to Pustylnick [2009].

Identity theft victims in the U.S. spend on an estimated average $1,500 and almost 200 hours in order to resolve the problems caused by such identity thieves [Yehuda 2014]. According to Yallapragada, Roe, and Toma [2012], one in three American households are victims of fraudulent crimes in technological-based environments.

The U.S. Computer Fraud and Abuse Act (CFAA) from 1986 define the following activities as fraudulent: accessing a computer to defraud and obtain value; intentional access and damage; trafficking in passwords; trespassing a computer; and economic espionage. Pustylnick [2009] adds that in the pre-Internet era, since there were no public network-access points, it was simple to guard information by passwords. In the following decades, computer-based environments became much more sophisticated as well as the type of fraudulent crimes against these infrastructures.

The 2009 ITU toolkit for cybercrime legislation [ITU 2009] manifests these changes; among the newly-defined electronic fraudulent crimes are the following acts: unauthorized access to computers, computer systems, and networks; unauthorized access to or acquisition of computer data and content data; interference and disruption; interception; misuse and malware; digital forgery; digital fraud, procure economic benefit; extortion; aiding, abetting, and attempting; and corporate liability. Pustylnick [2009] also points out that currently, many computer-based fraudulent activities are based on the theft of information, such as identification details or corporate information for verification purposes, such as addresses, phone numbers, and driver license numbers. Personal information required for fraud may also be attained by using virtual viruses, rootkits, and worms to damage organizational computerized systems.

3. Accounting Fraud

Fraudulent financial statements can cause massive losses among companies and individuals. There is a great need to understand the depth and the implementation of fraud prevention and detection technologies these scams. Accounting fraud are increasing and the identification and prevention is a subject of great importance among academic research and various industries.

3.1. GAAP and accounting fraud prevention

Kennedy [2012] notes that there are two possible reasons for inaccuracy of accounting records: error or fraud. Fraud is intentionally committed in order to render some gain for the perpetrator. The two means through which fraud is committed are:

Misappropriation of assets which refers to an incident when company assets (cash, inventory or fixed assets) are stolen or being used by an employee in an unauthorized way.

Misrepresentation of financial statements which occurs when financial statements are intentionally misstated. This may involve increasing reported revenues, decreasing reported expenses, or misrepresenting balance sheet accounts in order to change financial ratios to look more favorable, or reporting amounts differently from what would have been reported under GAAP (Messier 111). Misrepresentation may occur due to defalcation and similar irregularities, due to deliberate misrepresentation by management, or both.

Ball [2009] notes that the conviction in accounting profession (including the Financial Accounting Standards Board – FASB, a successor to the Accounting

Principles Board – audit firms, researchers and educators), was that financial reporting compliance with rules-based GAAP is sufficient to prevent fraud, while reality has shown that in several scandalous cases (Enron in particular), investors were misled by financial statements that were in technical compliance with GAAP but that did not reflect the economic substance of the transactions they were reporting.

3.2. The impact of accounting frauds

The direct impact of fraud is the financial loss due to theft or embezzlement. PWC's 2016 Global Economic Crime Survey, indicates that "Nearly a quarter (22%) of the survey respondents experienced losses of between $100,000 and $1 million, 14% of respondents suffered losses of more than $1 million, and 1% of respondents (primarily from North America and Asia-Pacific) reported losses in excess of $100 million. These are substantial sums of money and are representative of a trend of rising costs of individual frauds".

Accounting fraud may also impact non-fraudulent competitors. Sadka [2006] notes that Sadka [2004, 2005] has provided supporting evidence that competitors can use financial statements to extract the competitive advantage of a firm in the industry. when a firm falsely reports a competitive advantage, the competing firms might mistakenly choose a non-profitable investment and/or non-optimal firm organization in response. Armstrong claims in the Wall Street Journal that the accounting fraud of WC made ATT make bad investment decisions,

Financial fraud has a significant effect of environment. According to Sadka [2006], a firm that engages in accounting fraud will affect the whole industry and social welfare as well. The existing literature on accounting fraud finds that accounting fraud has a significant effect on financial markets. False financial reporting can result in overpriced securities and over borrowing by a firm. Since most debt contracts are based on accounting figures, manipulating these figures would help firms avoid bankruptcy and/or take on additional low-interest debt at the expense of the debt holders

Financial fraud may also effect the product market – Sadka [2006] notes that since a fraudulent firm will act in a non-optimal manner, accounting fraud is bound to affect the other firms in the industry, as the pricing (output) of one fraudulent firm's product will affect the prices (output) of the other firms' products.

An example to the effect that an accounting fraud may have on environment is "The Enron Effect" which was investigated by many researchers. Weaver [2004] notes that Enron's collapse, resulted in a lack of trust in corporate enterprise and markets. A 2002 poll showed only 16 percent of Americans trusted what any big company told them.

For all these reasons, firm managements and economics see the problem of detecting *and* preventing fraud as extremely important in sustaining a viable financial system. It has been addressed by several possible solutions – among them are increased regulation, increased transparency in financial reporting, and the uses of IT tools, as described later in this article.

3.3. Accounting fraud prevention

A survey was conducted on "The efficacy of regulation to prevent frauds and embezzlement in accounting". The purpose of the questionnaire was to investigate the attitudes of respondents about the role and impact of regulation in preventing fraud and embezzlement in accounting, compared to other **approaches and advanced technologies** that are not related to legislation and regulation, which are believed to reduce fraud. The survey examined the degree of participants' openness concerning accounting information provided by the companies reporting, as well as about the increasing degree of transparency, which can be equally effective approach.

The survey investigated the research questions using a combination of quantitative research (open interview questions) and quantitative research (closed questions). The quantitative and the qualitative research were each geared to answering distinct research questions. The decision to employ multi-strategy was taken in order to obtain diversity of views, and obtain qualitative evidence that would help to explain some of the relationships uncovered through the analysis of the survey data. The combined quantitative and open interview questions totaled to 49 questions. The decision to employ multi-strategy was taken in order to obtain diversity of views, and obtain qualitative evidence that would help to explain some of the relationships uncovered through the analysis of the survey data.

The survey covered 120 respondents from around the world, mostly Accountants, Comptrollers, Business managers, CFO and Auditors from: Profit Corporation, Accounting Firm, and Government, Not for Profit Organization. Therefore, the study measures a representation of a respected population from the members of the accounting profession around the world. The survey was uniform for all the participants and each participant has an equal chance of selection. The positions of the professionals in the sample range from CFOs, audit partners, auditors, audit managers, CPAs, directors of finance, directors of financial reporting, business managers, controllers, treasurers, accounting managers, accounting supervisors, senior accountants, staff accountants, to entry-level accountants.

The overall response rate for the survey was about 22%, which is considerable and comparing to the ranges of response rates reported by several recent surveys of financial executives. According to Graham, Harvey, and Rajgopal

[2005], Trahan and Gitman [1995] report a response rate of 12% in a survey mailed to 700 CFOs, while Graham and Harvey [2001] obtain a 9% response rate for 4,400 faxed surveys. Brav, Graham, Harvey, and Michaely [2004] have a 16% response rate. Of the 120 usable responses, approximately 58.5% of the survey participants were males. 41.5% are females, and 50.5% were from the Middle East. Overall, a majority the participants – 66.4% of the sample population – were employed in business organization, and 38.6% of the participants were employed by organizations with more than 500 employees. A majority the participants – 52.2% – have answered the survey questions based on experience. 47.8% of the participants are not experienced and have answered the survey questions based on their views and knowledge.

However, it should be noted that even though each industry experiences specific types of fraud that reflect some of their inherent business practices, the survey did not have different questionnaires tailored to the industries in the survey sample, with questions about the particular types of fraud experienced by their business establishment

In the open interview questions, respondents were asked to address the following questions:

A. What other measures or procedures can they mention concerning fraud risk in general?

Table 1 presents the responses by category on this question:

- 5 from 34 respondent's answers that Technology Solutions are the critical success factor for reducing frauds risk,
- 9 from 34 respondents' answer that audit process improvement.

Table 1. Success factors for reducing frauds risk

Respondents	Factor\tool	Category
2	Management's attitude towards the issue of fraud	organizational culture
4	Editing code of ethics in the organization	
2	Setting realistic goals for employees	
3	Transparency	
6	Increasing punishment	legislation and regulation
9	Audit process improvement	
5	Technological solutions	other
1	Strengthening Corporation	
2	Significant Increase of salaries	

Total = 34.

B. What are in their opinion the biggest problems in preventing accounting fraud?
   - 4 from 75 respondents claimed that reason is because of "Outdated technology" and that is the critical success in preventing accounting fraud,
   - 9 from 75 respondents' answer that audit process improvement.

Table 2. The major problems in preventing accounting fraud

Respondents	Factor\tool	Category
7	Lack of transparency	organizational culture
6	Lack of management involvment	
3	No cooperation teams	
11	No Moral values	
11	Management encourages cheating	
9	There is no cooperation with external audit	legislation and regulation
3	The lack of punishment	
1	Maintaining the independence of the organization	other
2	Lower rates of fraud detection	
4	Lack of professional and skilled	
3	Lack of resources allocation to tackle the problem	
4	Will meet market expectations	
1	Replacing stuff too often	
4	Outdated technology	
2	There are allso external frauds	
4	Unable to completely prevent fraud	

Total = 75.

Table 2 shows the tendency of respondents in ways that can minimize the incidence of fraud and risks, which believes a significant percentage of advanced technologies and other approaches will be very helpful.

4. Types of fraud

The two common types of fraud in a corporation are corporate fraud and management fraud. **Corporate fraud** refers to the embezzlement by internal factors within the company and possibly even external factors that damage the firm's financial situation. **Management fraud** refers to an act of embezzlement performed by the management towards external factors, primarily so as to maintain the company's status.

4.1. Corporate fraud

Several types of fraud in a company derive from internal risks in a business corporation.

Computerized fraudulence occurs when someone tampers with the input or with the output of data. **Input tampering** is based on the input of falsified data into the computer for personal purposes by the embezzler. For example, a fictive supplier or a fictive worker is inputted and payments are sent to the bank account of the embezzler who input the fictive data. **Output tampering** includes the theft of different types of output data on different media forms; for example, strategy programs, research and development programs, etc.

Computerized fraud can also be classified by the source of the fraud: **External fraud** is the most common type of fraud as systems are entered or "hacked". In some cases, the main damage is to the company's image and the theft of computer time, but some hackers break into a system so as to cause harm and use a system in order to obtain a financial benefit. External agents, such as suppliers or clients may threaten the organization by fraudulence acts. Suppliers may exploit the lack of supervision by double-billing or by submitting invoices that deviate from the original agreement as a way to charge unjustified amounts.

Internal frauds are committed by insiders who belong to the organization and receive a username, password and authorizations in a formal and recognized manner in order to perform their role. Fraudulence may occur also by payroll administrators and accountants that hold key positions, which enable them to falsify book records and conceal the embezzlement. These key-role employees can take royalties from clients by recording of discounts, credits, or bad debts or by recording false journal entries. A change of a supplier's bank-account information to the employee's relatives' bank-account information as the bank-clearing system performs the payment according to a bank account number without the verification of the supplier's name. Theft of clients' money may be concealed by sending false balance statements to clients**,** when the authorized employee has access to withdraw money from the client's accounts. The case of the Israeli bank employee Eti Alon and the affair in the City Bank of Switzerland are one example of this type of fraud, in which an authorized worker stole clients' money and sent false balance statements [*Globes* 2006]. Theft through forgery of checks may be concealed by producing false records in the bank adjustments. Payroll accountant may add fictive workers to the list of employees and, thus, may draw a salary from the organization's salary system in the name of the fictive employees. They may also inflate salaries of other related workers and share the difference with these workers, or approve continued payment for workers who previously left the organization and deviate the payment to the embezzler.

Another variation of this type of fraud involves both external and internal factors. This combined fraud consists of an employee in the organization, who cooperates with an outsider, who knows how to break through the authorization barrier.

Lendez and Korevec [1999] add that the managerial style impact on organizational behavior as whole. In organizations in which the management follows a philosophy of integrity and behaves according to high ethical values, employees will be less likely to conduct fraudulent acts, since it will not be tolerated. However, if organization managers ignore these moral rules in favor of achieving organizational goals at any cost, employees will be more likely to commit fraudulent acts as well.

4.2. Management fraud

When fraudulence occurs in the managerial level, the fraud is directed to external factors such as stockholders, financial institutions, tax authorities, the public, and investors. The embezzlements can be for the good of the company, so as to preserve its standing as a live business. The damage to the firm, if at all, is indirect in this case. A company must manage its books and report according to GAAP (Generally Accepted Accounting Principles). However, many managers see these principles as an obstacle to remove and not as a standard according to which managers should comply [Bilu and Peyt 2006]. Manipulations in the accounting methods' change and the inventory methods' change, as well as different reductions and estimates, may significantly affect the bottom line of net profit summary in the organization's financial report. Ball [2009] defines fraudulent financial reporting as knowingly failing to comply with GAAP, and mentions that as opposed to negligence, proving fraud requires establishing intentional wrongdoing.

Ball [2009] notes that managers face a variety of financial incentives to meet performance expectations. These include: gaining earnings-based bonuses; increasing their promotion prospects; avoiding termination; avoiding a decline in the value of their stocks, stock appreciation rights, and options; avoiding a downgrade of the company's debt, which could result in higher borrowing costs and further reductions in earnings; avoiding debt covenant violations that could lead to restrictions on dividend payments, new investment and further borrowing, or accelerated debt repayment; avoiding corporate bankruptcy; and hiding some other fraud (e.g., stolen assets, including cash).

4.3. The fraud triangle theory

As the review in this section demonstrates, fraudulence acts in organizations are committed both at the managerial level and the organizational level. The fraud triangle theory suggests that embezzlements take advantage of different incentives and opportunities. By rationalizing the fraudulence act, they enable the act. Lou and Wang [2011] suggest that the fraud triangle indicates pressure or incentive to perpetrate fraud, opportunity to carry out the fraud, or attitude/rationalization to justify fraudulent action. Such events or conditions are referred to "fraud-risk factors." Although these fraud-risk factors do not necessarily imply the existence of fraud, they often are present in circumstance where fraud existsAccording to Lou and Wang [2011] Pressure or incentive to commit fraud results from a perceived pressure on managers or employees to commit fraud. A firm may hold incentives to manipulate earnings, when financial stability is threatened by economy and industry, when management is pressured for meeting expectations of third parties, or when management or directors' personal financial situation is intimidated by the entity's financial performance. Opportunities result from circumstances that provide chances to commit fraud. Complicated transactions are accompanied with high inherent risk because of involvement in high degree of management judgment and subjectivity. Also, complicated transactions may present risks of material misstatement due to fraud because of susceptible to manipulation by management. Attitude or character is what leads one or more individuals to rationally commit fraud. Management integrity (attitude) is a major determinant of financial statement quality. When manager integrity is queried, reliability of financial statement is doubtful.

5. Accounting in IT environment

The proliferation of computer-based resources opened the door for a new kind computer crime and computer fraud [Kunz and Wilson 2004]. More organizations offer computer-based services by using telecommunications and Internet. These computer-based technologies raise some new challenges to the business world, from technology adoption dilemmas to financial limitations. Moreover, with the implementation of new technologies, increases the fear from privacy invasion, vulnerability, and online exposure, as stated by Kabir Usman [2013].

The issue of security is linked to fraudulent activities as a result of the weakness of the internal control systems. As demonstrated in the following pages, security in computer-based environment may be improved by applying certain organizational policies and control mechanisms, conducting transparency and better supervision on authorized employees, as well as on managers. Fraud-detection software may contribute as well to minimize the number of fraud cases in the business world.

As mentioned above, in the U.S. alone, it is estimated that victims may spend on average $1,500 in out-of-pocket expenses and an average of 175 hours in order to resolve the various problems caused by fraud and identity thieves. Organizations that engage in e-commerce to a large extent need to protect their customers against these crimes. An empirical study of 75 managerial employees and/or knowledge workers in five large organizations in Pittsburgh, PA, revealed a number of interesting facts in regards to how much information employees share with others, to the likelihood of conducting business online, and to whether or not these employees would take preventive steps to protect their personal identity and credit. The study offered a model to calculate the implications of such preventive steps by employees and customers in order to avoid identity theft [Smith and Lias 2007].

6. IT tools existing in the accounting area

6.1. Data mining

Data mining investigates large populations of data and provides useful response which can be easily interpreted by auditors. Data mining uses a set of techniques that help to find and collect vital information that may lead to fraud detection [Almeida 2009]. Data mining techniques can assist in identifying fraudulent financial accounting, since dealing with large data volumes and complexity of financial data are the major challenges in forensic accounting. Panigrahi and Sharma [2012] claim that Data mining based financial fraud detection automates the entire process of scanning and testing of various reports.

Data mining can assist in detecting both external and internal computerized corporate fraud, such as Input tampering which is based on the input of falsified data into the computer for personal purposes by the embezzler. This is enabled by the ability of data mining tools to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. Fraudulence by payroll administrators and accountants that hold key positions, may be detected by data mining tools. Recording of discounts, credits, or bad debts by booking false journal entries, changing of a supplier's bank-account information, adding of fictive workers to the list of employees or fictive supplier to the list of suppliers – can all be detected by data mining tools and techniques.

Almeida [2009] note that the ultimate goal of applying data mining to fraud detection is to create a classification model that can label a record, person or company as being fraudulent or not. These methods could assist auditors in accomplishing the task of management fraud detection because they have advanced classification and prediction capabilities [Kirkos, Manolopulos, and Spathis 2007].

Below is a list of the most popular programs of data mining [Emanuel 2013]:[3]

1. IBM SPSS Modeler – has a visual interface that allows users to leverage statistical algorithms and data mining algorithms without the need for programming. The software enables automatic classification, automatic grouping, anomaly detection, list decisions, discrimination, and regression and so on. IBM SPSS Modeler can assist in fraud prevention and detection by:
   a. Identifying Vulnerabilities – the system can estimate exposure and Probe weakness. The system can detect insider threat and predict fraudulent activities. Entity analysis abilities enable the system to Identify leads and Process referrals. Predictive Modelling Find Threat and Fraud patterns in the data;
   b. Detect Transactions – IBM SPSS Modeler can create and execute models that are "normal". The system will generate smart business rules based on statistical scoring. Rules and models will be integrated with the business operating system. The system will take a direct and pre-emptive action as it will be able to identify and intercept suspicious actions. Anomaly detection abilities will assist in Identifying new and emergence fraud patterns;
   c. Evaluate Workload – Screen leads Select leads Prioritize cases;
   d. Scoring, Reporting/Dashboard, Model Management – the system monitors metrics, ensures performance and provides insights to front-line managers and executives. Analysis of data post event will enable managers to refine policy.
2. SAS Data Mining – provides algorithms and models for forecasting and modeling descriptions, in order to simplify and streamline the data mining technique to find the model that gives the best results. Features include an array of data preparation tools, dimensional reduction techniques, visualization and interactive exploration, advanced models, development models, automated process for giving the score and scalable processing.

   SAS helps organizations to detect and manage fraud in a proactive way, based on the integration of many different approaches to fraud detection. The system can detect anomalies using a wide range of approaches, including analytical visualization for univariate and multivariate outlier detection, anomaly detection based on time series data, dynamic profiling, and cluster analysis for outlier detection

   One technique to test the distribution of monetary amounts that might be suspected to be fabricated by a fraudster using analytical visualization is that based on the plausible assumption that people who make up figures tend to distribute their digits fairly uniformly, a simple comparison of the

[3] http://www.predictiveanalyticstoday.com/top-data-mining-software/.

first-n-digits frequency distribution from the data with the expected distribution is likely to reveal any anomalous results

Most of the data points follow the predicted pattern; when one point shows a substantial deviation. With the use of time series analysis techniques, the system is able to take seasonal patterns into account for identifying deviations from the norm. Organizations may have business rules for detection of abnormalities on predefined metrics. If the threshold implemented with the business rule is exceeded, the rule would create an alarm in the process. However, these rules tend to be rather static and do not take observed fluctuations into account. The system enables the uses of regular time series analysis combined with forecasting can automatically take these natural fluctuations into account.

If no target for confirmed fraud is available from the data, the data attribute under investigation can be modeled using predictive modeling techniques and outliers can be detected using the residuals. The system enables organizations to define a measurement that identifies the extreme residuals, such as the three standard deviations percentile, and mark all residuals that exceed this threshold for further investigation.

Techniques like link analysis, association analysis, and path analysis can help to uncover relationships within the organization that point to suspicious behavior and indicate that a group of people may be working together to execute fraudulent activities.

3. RapidMiner – provides an integrated environment for machine learning, data mining, text mining, analytical forecasting and business analytics. Used business and industrial applications, research, education, training, and application development.

   Vadoodparast and Hamdan [2015] concluded that "The KDA model in Rapidminer software could improve consuming time processing and make three customer modeling in the same time to help detection suspicious transaction in customer side better. Developed FDS and DSS software can highlight and then classify the transaction with result of modeling. The accuracy obtained by KDA modeling is 68.75% for dynamic online modeling and 81.25% for historical or offline modeling and seemed it is competitive with other algorithms in this area".

   Rapidware offers a large range of anomaly detection methods and introduces the RapidMiner Anomaly Detection Extension. Anomaly detection is the process of finding patterns in a given dataset which deviate from the characteristics of the majority. Application domains among others include network security, intrusion detection, computer virus detection, fraud detection, misuse detection, complex system supervision, and finding suspicious records in big data, including industry-specific applications.

   According to Amer and Goldstein [2012], Unsupervised anomaly detection is the process of finding outlying records in a given dataset without prior need for training. An anomaly detection extension for RapidMiner assists non-experts with applying eight different nearest-neighbor and clustering based algorithms on their data. An anomaly detection extension for RapidMiner contains the most well-known unsupervised anomaly detection algorithms. This extension will enable analysts to use those algorithms and integrate the operators into more complex processes easily

4. Microsoft Analysis Services – builds analytic models featuring multi-dimensional models that can be used for interactive data analysis, reporting and visualization.
5. Oracle Data Mining – provides functional data mining using SQL functions in a foreign Oracle database, enabling users to discover new insights hidden data.

6.2. ERP (Enterprise Resource Planning Software)

Enterprise Resource Planning systems provide complete automation of the business processes of an organization. Users within the organization operate the system to carry out day-to-day transactions such as financial, HR, and inventory transactions. Nevertheless, although ERP systems provide safeguard procedures, such as Segregation of Duties (SoD) to prevent fraud, they are still vulnerable and require additional fraud detection mechanism, as claimed by Islam et al. [2010].

"With increased use of technology, it has become necessary to audit through the computer," claim Byington et al. [2003]. An auditor must keep in mind "that the tool used to detect illegal activities is the same tool used to commit many of the crimes"[Byington et al. 2003].

Khan, Corney, Clark, and Mohay [2010] propose a set of (1) anomaly types to detect potentially suspicious user behavior, and (2) scenarios to identify inadequate segregation of duties in an ERP environment. Khan et al. [2010] adapted a role mining approach for generating transaction profiles from the user activities recorded in the security log of an ERP system, and for identifying subset relationships amongst such transaction profiles, and have postulated a number of anomalous, possibly fraudulent, activity scenarios which can be detected using the transaction profiles. They have identified such anomalies have implemented scenarios that identify violations in proper segregation of duties and have detected such violations using the transaction profiles generated.

Thus, similar to data mining, ERP can assist in detecting both external and internal computerized corporate fraud, such as Input tampering, by using its ability to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles.

Islam et al. [2010] have demonstrated in their work that ERP can assist in detecting corporate fraud such as Redirected vendor Payment (when payment is made in such a way so that the payment goes not to the vendor's actual account but to a re-directed account), False Invoice Payment (when The intention of this fraud is to make a false payment for one's own benefit), Misappropriation (purchase order and purchase approval by the same user). Using the developed prototype software Islam et al. [2010] successfully tested the detection of all scenarios described in their paper on synthetically generated transaction log data, showing the possibilities of ERP systems to provide fraud detection and prevention.

Flegel, Vayssière and Bitz [2010] mention the functionalities embedded in ERP software, such as the Auditing Information System (AIS) provided by SAP ERP. It is a set of reports that an auditor can run to generate the information most needed in financial audits and fraud audits. Among those reports are fraud-specific ones such as multiple invoices, one-time vendor accounts and analysis of payment terms.

6.3. EMAIL

Email correspondence is arguably the most common form of electronic evidence [Albrecht 2006] but there are surprisingly few advanced email technologies that take advantage of the large amount of information present in a user's inbox [Bekkerman et al. 2004]. Keila and Skillicorn [2005] found that the use of some exclusive words could suggest that the story is fictitious .Based on their findings, their approach ranked emails by how likely they were to be deceiving.

6.4. Extensible Business Reporting Language software (XBRL)

The Extensible Business Reporting Language is developed to enable users of financial reports to read, analyze, and compare between reports published in different languages and in different countries easily and efficiently; and to enable in the long-run the publishing of financial reports in real time. XBRL enables automated comparison and analysis of reports, and easy comparison of financial and operational relations of companies throughout the world. XBRL is able to :

- Provide a database-like structure, using text files,
- Define a collection of financial facts for a specific report, industry, and jurisdiction (taxonomy),
- Facilitate the data exchange between proprietary systems,
- Promotes the re-use of data with far less effort.

Regulators, professional organizations, and financial reporting standards-setters around the globe look at interactive data as a way of promoting the transparency of financial information and monitoring of corporate reporting [Roohani, Furusho, and Koizumi 2009]. To achieve a higher degree of transparency, corporate disclosures should be timely, clear and contain all information that will impact materially on the company [Hannon 2002]. XBRL may be helpful as it can provide an electronic method for reporting financial information in accordance with generally accepted accounting principles (GAAP). In addition, tax filings, SEC reports, disclosures to the financial press, and internal reports can be quickly and easily prepared, sent, and loaded directly into analytical programs by analysts [Hannon 2002].

As of 2012, public companies in the U.S. are required by the U.S. Securities and Exchange Commission to submit financial reports with XBRL tags, so that corporate financial data can be rapidly searched and analyzed. Sheridan and Drew [2012] noted that accurate use of XBRL requires users who are also familiar with accounting standards, and that individuals with both sets of skills are rare and in great demand, The use of XRBL may lead to educating for values of transparency, which will therefore prevent the phenomenon of asymmetric information and enable easy access to information in an objective situation; thus, preventing ahead of time fraud and embezzlement attempts.

By increasing transparency, comparability and accessibility of financial data which are enabled by the use of XBRL, can assist in detecting management fraud which is directed to external factors such as stockholders, financial institutions, tax authorities, the public, and investors. Manipulations in the accounting methods' change and the inventory methods' change, as well as different reductions and estimates, and reports that do not comply with GAAP, are easier to detect when using XBRL.

Conclusions

This research aimed to explore the tools and the different ways of utilizing current technology to assist auditors and the auditing environment in improving fraud deterrence and detection. Analysis of this research is included three principal aspects: the current IT environment and the role of auditing in this context; definitions of fraud and threats; and different approaches to detect frauds.

In today's technological-based environment, many traditional common control mechanisms no longer exist. The auditor has to adapt to the growing paperless-business environment, in which highly-complex computer software – Enterprise Resource Planning (ERP) systems – is responsible for electronically sending, receiving, and storing this information. As previously stressed, auditors should be able to monitor these complex ERP systems in order to identify and prevent frauds.

Frauds may occur on the corporate level or the managerial level; they may be induced by internal authorized or unauthorized employees, external factors such as suppliers, or both. Auditors should use the different technological tools available to them in order to detect these acts of embezzlements: monitoring the emails of employees, using XBRL in order to report financial information, or applying Open-Book Accounting (OBA) policy in the organization in order to be transparent to clients and the authorities. Moreover, as a set of aspired ideals for transparent corporative behavior, OBA could be used to understand inter-organizational relationship and the value created by the interfirm economic space.

References

Albrecht, C.C., Albrecht, W.S., Dunn, J.G., 2006, *Can Auditors Detect Fraud: A Review of the Research Evidence. 2001*, Journal of Forensic Accounting, vol. 2: 1–12.

Almeida, M.P.S.-B., 2009, *Classification for Fraud Detection with Social Network Analysis*, Dissertation, Engenharia Informatica e de Computadores.

Amer, M., Goldstein, M., 2012, *Nearest-neighbor and Clustering Based Anomaly Detection Algorithms for Rapidminer*, *Proc.* of the 3rd RapidMiner Community Meeting and Conference (RCOMM 2012): 1–12.

Ball, R., 2009, *Market and Political/Regulatory Perspectives on the Recent Accounting Scandals*, Journal of Accounting Research, 47(2): 277–323.

Chan, Y.D., Vasarhelyi, M.A., 2011, *Innovation and Practice of Continuous Auditing*, International Journal of Accounting Information Systems, 12 (2011): 152–160.

Flegel, U., Vayssière, J., Bitz, G., 2010, *A State of the Art Survey of Fraud Detection Technology*, Insider Threats in Cyber Security, Springer US: 73–84.

Hake, E.R., 2005, *Financial Illusion: Accounting for Profits in an Enron World*, Journal of Economic Issues, vol. 39(3): 595–611.

Hannon, N., 2002, *Accounting Scandals: Can XBRL Help?,* Strategic Finance, 84. 2: 61–62.

Islam, I.A., Corney, M.W., Mohay, G.M., Clark, A.J., Bracher, S., Tobias, R., Flegel, U., 2010, *Fraud Detection in ERP Systems Using Scenario Matching*, Security and Privacy: Silver Linings in the Clouds. Brisbane Convention and Exhibition Center, Australia.

Jones, M.J., 2011, *Creative Accounting, Fraud and International Accounting Scandals*, John Wiley & Sons.

Kabir Usman, A., 2013, *Critical Success Factors for Preventing E-banking Fraud,* Journal of Internet Banking and Commerce, 18 (2): 1–16.

Keila, P.S., Skillicorn, D.B., 2005, *Detecting Unusual and Deceptive Communication in Email*, Centers for Advanced Studies Conference: 17–20.

Kennedy, K.A., 2012, *An Analysis of Fraud: Causes, Prevention, and Notable Cases*, http://scholars.unh.edu/cgi/viewcontent.cgi?article=1099&context=honors.

Khan, R.Q., Corney, M.W., Clark, A.J., Mohay, G.M., 2010, *Transaction Mining for Fraud Detection in ERP Systems*, Industrial Engineering and Management Systems, 9(2), in Press.

Kirkos, E., Manolopoulos, Y., Spathis, C., 2007, *Data Mining Techniques for the Detection of Fraudulent Financial Statements*, Expert Systems with Applications, vol. 32: 995–1003.

Kotsiantis, S., Koumanakos, E., Tampakas, V., Tzelepis, D., 2006, *Forecasting Fraudulent Financial Statements using Data Mining*, International Journal of Computational Intelligence, vol. 3, no. 2.

Kunz, M., Wilson, P., 2004, *Computer Crime and Computer Fraud*, College Park: University of Maryland, Department of Criminology and Criminal Justice.

Lendez, A.M., Korevec, J., 1999, *How to Prevent and Detect Financial Statement Fraud,* The Journal of Corporate Accounting and Finance, 11(1): 47–54.

Lou, Y.I., Wang, M.L., 2011, *Fraud Risk Factor of the Fraud Triangle Assessing the Likelihood of Fraudulent Financial Reporting*, Journal of Business & Economics Research (JBER), 7(2).

Panigrahi, P., Sharma, A., 2012, *A Review of Financial Accounting Fraud Detection based on Data Mining Techniques*, International Journal of Computer Applications (0975–8887), vol. 39, no. 1.

Pustylnick, I., 2009, *Financial Data Set Used is Computerized Fraud Detection*, Swiss Management Center, Transknowlogy Campus.

Roohani, S., Furusho, Y., Koizumi, M., 2009, *XBRL: Improving Transparency and Monitoring Functions of Corporate Governance*, International Journal of Disclosure and Governance, 6, November: 355–369.

Sadka, G., 2006, *The Economic Consequences of Accounting Fraud in Product Markets: Theory and a Case from the US Telecommunications Industry (WorldCom)*, American Law and Economics Review, 8(3), 439–475.

Sheridan, B., Drew, J., 2012, *The Future Is Now: XBRL Emerges as a Career Niche*, Journal of Accountancy (June): 123–127.

Smith, A.D., Lias, A.R., 2007, *Identity Theft and E-Fraud Driving CRM Information Exchanges*, Hershey, PA: IGI Publishing.

The Real Time Economy, 2002, Economist.

Vadoodparast, M., Hamdan, A.R., 2015, *Fraudulent Electronic Transaction Detection Using Dynamic KDA Model*, International Journal of Computer Science and Information Security, 13(3): 90.

Yallapragada, R.R., Roe, C.W., Toma, A.G., 2012, *Accounting Fraud, and White-collar Crimes in the United States*, Journal of Business Case Studies, 8(2): 187–192.

Aims and Scope

Economics and Business Review is the successor to the Poznań University of Economics Review which was published by the Poznań University of Economics and Business Press in 2001–2014. The Economics and Business Review is a quarterly journal focusing on theoretical and applied research work in the fields of economics, management and finance. The Review welcomes the submission of articles for publication dealing with micro, mezzo and macro issues. All texts are double-blind assessed by independent reviewers prior to acceptance.

Notes for Contributors

1. Articles submitted for publication in the Economics and Business Review should contain original, unpublished work not submitted for publication elsewhere.
2. Manuscripts intended for publication should be written in English and edited in Word and sent to: secretary@ebr.edu.pl. Authors should upload two versions of their manuscript. One should be a complete text, while in the second all document information identifying the author(s) should be removed from files to allow them to be sent to anonymous referees.
3. The manuscripts are to be typewritten in 12' font in A4 paper format and be left-aligned. Pages should be numbered.
4. The papers submitted should have an abstract of not more than 100 words, keywords and the Journal of Economic Literature classification code.
5. Acknowledgements and references to grants, affiliation, postal and e-mail addresses, etc. should appear as a separate footnote to the author's name[a, b, etc] and should not be included in the main list of footnotes.
6. Footnotes should be listed consecutively throughout the text in Arabic numerals. Cross-references should refer to particular section numbers: e.g.: See Section 1.4.
7. Quoted texts of more than 40 words should be separated from the main body by a four-spaced indentation of the margin as a block.
8. Mathematical notations should meet the following guidelines:
   - symbols representing variables should be italicized,
   - avoid symbols above letters and use acceptable alternatives (Y*) where possible,
   - where mathematical formulae are set out and numbered these numbers should be placed against the right margin as... (1),
   - before submitting the final manuscript, check the layout of all mathematical formulae carefully (including alignments, centring length of fraction lines and type, size and closure of brackets, etc.),
   - where it would assist referees authors should provide supplementary mathematical notes on the derivation of equations.
9. References in the text should be indicated by the author's name, date of publication and the page number where appropriate, e.g. Acemoglu and Robinson [2012], Hicks [1965a, 1965b]. References should be listed at the end of the article in the style of the following examples:

   Acemoglu, D., Robinson, J.A., 2012, *Why Nations Fail. The Origins of Power, Prosperity and Poverty*, Profile Books, London.

   Kalecki, M., 1943, *Political Aspects of Full Employment*, The Political Quarterly, vol. XIV, no. 4: 322–331.

   Simon, H.A., 1976, *From Substantive to Procedural Rationality*, in: Latsis, S.J. (ed.), *Method and Appraisal in Economics*, Cambridge University Press, Cambridge: 15–30.
10. Copyrights will be established in the name of the E&BR publisher, namely the Poznań University of Economics and Business Press.

More information and advice on the suitability and formats of manuscripts can be obtained from:

Economics and Business Review
al. Niepodległości 10
61-875 Poznań
Poland
e-mail: secretary@ebr.edu.pl
www.ebr.ue.poznan.pl

Subscription

Economics and Business Review (E&BR) is published quarterly and is the successor to the Poznań University of Economics Review. The E&BR is published by the Poznań University of Economics and Business Press.

Economics and Business Review is indexed and distributed in ProQuest, EBSCO, CEJSH, BazEcon and Index Copernicus.

Subscription rates for the print version of the E&BR: institutions: 1 year – €50.00; individuals: 1 year – €25.00. Single copies: institutions – €15.00; individuals – €10.00. The E&BR on-line edition is free of charge.

Correspondence with regard to subscriptions should be addressed to: Księgarnia Uniwersytetu Ekonomicznego w Poznaniu, ul. Powstańców Wielkopolskich 16, 61-895 Poznań, Poland, fax: +48 61 8543147; e-mail: info@ksiegarnia-ue.pl.

Payments for subscriptions or single copies should be made in Euros to Księgarnia Uniwersytetu Ekonomicznego w Poznaniu by bank transfer to account No.: 96 1090 1476 0000 0000 4703 1245.