Spring 2012

Detecting fraud: Utilizing new technology to advance the audit profession

Gabriella Stanton
University of New Hampshire - Main Campus

Honors Thesis

Detecting Fraud:

Utilizing New Technology to Advance the Audit Profession

Spring Semester, 2012

Faculty Sponsor: Dr. Jake Rose

Table of Contents

Table of Figures

Background

The Sarbanes-Oxley Act was instituted in 2002 because of major fraud scandals throughout the U.S. Managers became responsible of ensuring the presence of adequate internal controls and improving the accuracy and reliability of financial reporting and disclosures, which would reduce the likelihood of and assign accountability to fraud (Keila et al. 2005, Kotsiantis et al. 2006). External auditors are also required to report on the effectiveness of these internal controls and evaluate management's assessments of the controls.

With new technological advances, many common controls and paper documents that were used to implement controls no longer exist. The role of an auditor is changing and needs to adapt to the increasingly paperless business environment. Gone are the days where pre-numbered documents helped account for the completeness of a transaction. Today, highly complex computer software, called Enterprise Resource Planning (ERP) systems, takes care of electronically sending, receiving, and storing this information.

Auditors need to be able to continuously monitor these complex ERP systems in order to identify and prevent problems before they occur. The availability of massive quantities of data in these new ERP systems also creates new opportunities for auditors. One of these opportunities is improved methods to detect fraud. Whether it is fraudulent financial reporting or misappropriation of assets, there are novel techniques being developed outside of accounting that auditors could employ to assess the likelihood and risk of fraud.

Objectives

Although much work has been done on text mining using the Enron Email Dataset (Keila et al. 2005), this thesis will explore other and more diverse ways of utilizing current technology to help auditors and the auditing profession improve the prevention and detection of fraud. The objectives of this thesis are as follows:

1. To describe the current business environment; why are audits necessary?
2. To define fraud; why worry about fraud?
3. To describe how fraud can be detected: past, present, and in the future?

Current Business Environment

In the current business environment, almost every instance of financial fraud is perpetrated with the use of a computer (Albrecht *White Paper*). The complexity that technology has created in this environment puts more responsibility on the auditor to use all available resources to ensure a thorough examination of accounting records (Byington et al. 2003). Hua et al. (2008) explain that "the main contributing factors to the prevalence of fraud are the growing complexity of organizations and systems, changes in business processes and activities, enormous and ever-expanding volumes of transaction data, and outdated and ineffective internal controls."

Audits of financial statements are a necessary "monitoring mechanism that helps reduce information asymmetry and protect the interests of the principals, specifically, stockholders and potential stockholders, by providing reasonable assurance that management's financial statements are free from material misstatements (Hunton et al. 2008)." Therefore it is critical for a financial statement audit that the auditor use the most up to date resources available in order to ensure the most effective and efficient audit.

What is fraud?

Accounting frauds can be categorized as being either fraudulent financial reporting, misappropriation of assets, or both (Kotsiantis et al. 2006). The Treadway Commission defines fraudulent financial reporting as intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements. Misappropriation of assets occurs when business assets and resources are not used for their intended purposes. Examples include thievery, cash skimming and embezzlement (Kotsiantis et al. 2006). Another classification of fraudulent financial reporting is management fraud which Kirkos et al. (2007) define as the deliberate fraud committed by management that causes damage to investors and creditors through material misleading financial statements.

The fraud triangle outlines three factors believed to be present in every fraud instance: incentive, opportunity and attitude (Skillicorn et al. 2007). We can ask the following questions in order to evaluate the environment using the fraud triangle:

How would an employee rationalize committing a fraud?

Does the culture of the organization promote ethical behavior?

Were there multiple occasions for an employee to commit fraud?

Was there an incentive that was presented?

Attitude refers to the integrity and the culture of the organization. It also involves "the propensity of the individual to rationalize the fraud (Skillicorn et al. 2007)." Wilks et al. (2004) note that opportunity results from "working conditions, including control deficiencies and/or management override that result in circumstances allowing fraud to occur." Incentive results from "a perceived benefit from committing fraud such as accounting-based bonuses or stock

options (Skillicorn et al. 2007)." When an opportunity to commit fraud presents itself and there is a large enough incentive, a fraud may still be perpetrated even if management's integrity is considered to be adequate.

Cullinan et al. (2006) explain that in a financial statement audit, there are three main ways that auditors can detect fraudulent misstatements:

1. Through the client's control system
2. Through the auditor's effective use of analytical review
3. Through substantive testing of transactions and balances.

However, Kotsiantis et al. (2006) note that detecting management fraud is a difficult task when using normal audit procedures since there is a shortage of knowledge concerning the characteristics of management fraud. Additionally, Kotsiantis et al. (2006) explain that given its infrequency, most auditors lack the experience necessary to detect fraud. Also, managers may deliberately try to deceive auditors. All three of these factors make it necessary to explore new and improved ways to detect and deter fraud in an organization.

Why worry about fraud?

Fraudulent financial reporting (FFR) has serious consequences for the organization and for the public's confidence in capital markets (Kotsiantis et al. 2006). The costs of fraud to US businesses are estimated to be more than $400 billion each year (Kirkos et al. 2007). Additionally, up to 6% of organizations' revenues may be lost annually as a result of fraud and abuse (Hua et al. 2008). This is even more worrisome because according to the results of KPMG's Fraud Survey of 2003, organizations are reporting more experiences of fraud than in prior years (Hua et al. 2008).

Byington et al. (2003) state that although all levels of business are involved, the greatest losses to fraud are found at the supervisory and executive level. This finding is confirmed in a detailed review of the SEC's accounting and auditing enforcement releases, which found that "the preponderance of financial statement frauds are perpetrated by the very top levels of management - generally the CEO or equivalent level (Cullinan et al. 2006)." The increased reliance on control assessment and analytical review by auditors and audit processes opens the possibility of more frauds being undetected, because of their focus on lower level employees, rather than top managers (Cullinan et al. 2006).

There are also costs associated with misclassifying a fraudulent transaction as non-fraudulent. This is known as a Type II error. The costs that result from Type II errors are much higher than Type I errors, which occur when a non-fraudulent transaction is classified as fraudulent.

Because of the technology boom, it is argued that unintentional financial statement error will diminish and that future demand for audits will "depend largely on their ability to detect or deter fraud (Skillicorn et al. 2007)." SAS Nos. 53 (AICPA 1988), 82 (AICPA 1997), and 99 (AICPA 2002) contain extensive lists of fraud risk cues. Checklists from these standards have been developed by auditors to ensure that each fraud risk cue is considered (Skillicorn et al. 2007). However, these checklists "fail to consider how management could manipulate the cues on the checklists (Skillicorn et al. 2007)." This failure to consider management's response prevents auditors from designing procedures that management does not anticipate. Wilks et al. (2004) also found that auditors who employ the fraud risk checklists are "*less* sensitive to fraud than auditors who do not use checklists."

Hua et al. (2008) note that fraud "is composed of the following three categories: intentional illegal act, the concealment of the act, and deriving a benefit from that act." Because fraudulent activities are usually well-planned and intentionally covered up, it is difficult for the auditor to detect these incidents. Although fraud does not happen as often as misuse and error, when it does occur, it usually represents a large amount that has been misstated.

Detecting Fraud

An audit can be designed to be done around the computer or through the computer. Auditing around the computer doesn't involve evaluating a client's computer controls. Documents are chosen at random and the auditor then verifies the resulting outputs of the system with the inputs. Therefore, this process assures that the controls must be working properly and effectively when outputs are correct. Before the integration of technology and the automation of many corporate accounting systems, "the audit was usually designed to go around the computer, but with increased use of technology, it has become necessary to audit through the computer (Byington et al. 2003)." But, as a caution, 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)."

Auditing through the computer involves evaluating the existence and effectiveness of the client's controls. This method is designed to test the automatic controls present in complex IT systems. In 2012 the latest version of COBIT (Control Objectives for Information and related Technology), COBIT 5, was released by the Information Systems Audit and Control Association (ISACA). COBIT 5 is a framework that lets managers connect control requirements, IT issues and risks associated with the business.

There are four techniques that can be used to audit through the computer, though test data is used most often. (Figure 1.)

(1) Test data

(2) Parallel Simulation

(3) Integrated Test Facility

(4) Embedded audit module

Test data Technique	**Uses a set of hypothetical transactions to audit the programmed checks and program logic in both transaction and nontransaction processing programs. The test data approach requires only a modest investment in time to apply in practice and does not require an extensive background in information technology.**
Parallel simulation	Attempts to simulate or duplicate the firm's actual processing results. To employ this technique, the auditor writes a computer program, using an audit software package, or using packaged accounting software, such as BusinessWorks, Oracle Financials, PeopleSoft Financials, M.A.S. 90 Evolution2 and SAP R/3. The auditor's objective is to use the software to input the firms actual data for a past period and generate the same output as the live production programs. The auditor's simulated results and the actual processing results are compared, and differences noted, investigated, and corrected.
Integrated test facility (ITF)	Enables test data to be continuously evaluated when transactions are processed by online systems. The auditor creates fictitious situations, such as a bogus department completing purchasing requisitions or purchase orders being sent to bogus vendors, and performs a wider variety of tests compared to the test data approach. The implementation of ITF is time-consuming and costly, requiring a high-level of computer expertise.
Embedded audit module	Is a programmed module or segment that is inserted into an application program. Its purpose is to monitor and to collect data based on transactions, particularly those processed by online computer-based systems. The data are then used by the auditor in the tests of controls and the evaluation of control risk. The application of this method requires the auditor to have a good working knowledge of computer technology, including computer programming.

Figure 1. Techniques used to audit through the computer
Source: Cerullo et al. 2003

Hua et al. (2008) highlight that data analysis is critical as a means of allowing auditors to "streamline audit processes, bring fraudulent activities to light before they result in critical losses, minimized financial losses, and ensure compliance with business rules and external regulatory requirements, such as SAS 410 and SOX ." In order to accomplish this, fraud

detection methods should use full populations whenever possible, and since full populations can be voluminous, they almost always require computers and data mining techniques (Albrecht *White Paper*). Thus, as Byington et al. (2003) point out, the computer is the most essential tool an independent auditor can utilize for the detection of fraud. The discovery of the WorldCom fraud is one example of "using computer technology to search full populations of data for anomalies, trends, and fraud (Albrecht *White Paper*)."

Much exploratory research into new methods of combining publicly-available company information could prove effective. Albrecht provides examples of publicly available external information that may prove useful in future investigation of frauds:

(1) Incorporation records

(2) Property and other asset records

(3) Civil lawsuits

(4) Tax liens

(5) Civil judgment records

(6) Bankruptcy filings

(7) Home values, loans, neighbor contact information

(7) News articles or current events

This information may be valuable in determining if upper management is engaging in questionable activities that might cause concern. Because Sarbanes-Oxley requires auditors to assess the attitude present at the top levels of the organization, risky external behaviors could be a red flag in an audit. In the end, research may show that financial statements are just too summarized for effective data mining for fraud (Albrecht *White Paper*).

ERP

Enterprise Resource Planning software has become a necessity in the current business environment. This is because "the development and pervasive use of ERP systems provides the critical infrastructure necessary for the effective evolution of the assurance function from a periodic event to an ongoing process through the integration of continuous auditing applications (Kuhn et al. 2010)." Bierstaker et al. (2001) found that more than 10,000 companies currently use some form of enterprise computing platforms such as SAP R/3.

ERP and Continuous Monitoring

The complexity of US business structures and systems often makes it difficult to eliminate errors from financial systems and to reduce employee misuse of assets or failure to comply with policies (Hermanson et al. 2006). The control environments of businesses also increase the applicability of continuous monitoring; if some employees or managers see that errors go undetected, this can open the door to misuse of the company resources or simple disregard for company policies. This makes it extremely difficult to oversee the actions of thousands of employees on a daily basis.

Hermanson et al. (2006) found that continuous monitoring can significantly reduce fraud, misuse, and errors. This can be achieved by using Enterprise Resource Planning (ERP) systems that provide companies with (1) much greater ability to process and manage information and (2) much greater monitoring/auditing capacity. Even with this greater ability and greater capacity, most companies have focused on the ability to process and manage more information, while monitoring/auditing capacity has received less attention. As a result, many organizations have large, unexplored databases that could yield important insights into the incidence of errors, misuse and fraud (Hermanson et al. 2006). This is important because early detection and

understanding root causes of problems are critical to reducing fraud opportunities and preventing losses of company assets (Hermanson et al. 2006).

Figure 2. shows a four component process for investigating possible fraud in the organization which would be led by the internal audit function. During continuous monitoring, alerts would be received by the internal audit team who would then determine if further investigation is necessary. If a formal investigation is required the team would notify the appropriate groups and then proceed to the Investigation Phase. This phase is comprised of obtaining evidence, evaluating report findings and performing any administrative, legal or other follow ups. An incident analysis would follow the formal investigation which would include reviewing for any links to other fraud incidents and for any patterns in the fraud. Finally the team would implement any corrective measures it found required. This process is necessary because of the complexity of fraud incidents. Continuous monitoring also can lead to cost savings in the Sarbanes-Oxley Section 404 arena (SOX 2002).

Continuous monitoring methodologies are increasingly viewed by internal audit as a means to enhance their audit processes as well as to meet stakeholder needs and their demands for faster and higher-quality real-time assurance (PWC 2006). In this role, continuous monitoring is designed to identify errors and wrong-doing early in the transaction process.

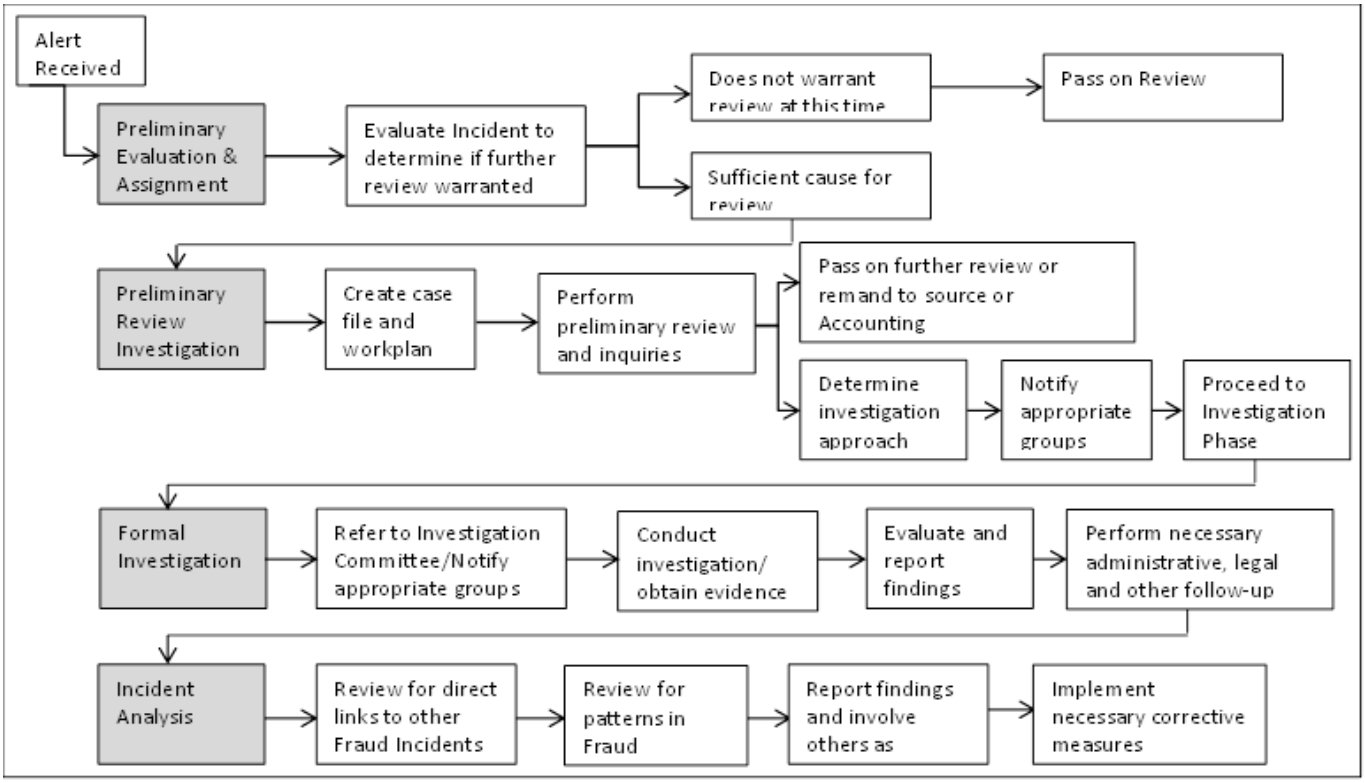

Figure 2. Response Process - Possible Fraud Process Flowchart
Source: Oversight Systems, Inc.

Behavioral Analysis

As mentioned earlier, fraud is composed of an intentional illegal act and the concealment of that act. Kotsiantis et al. (2002) emphasize the fact that "unintentional nonfraudulent financial statement errors are *static* in that their incidence is unaffected by the anticipated audit. But fraud is intentional and *strategic* such that its incidence is affected by the anticipated audit." Auditors need to be mindful that most managers know what to expect and can plan for an upcoming audit. When looking at email or any documented communication between employees, Keila et al. (2005) point out that "awareness that some kind of surveillance may be in place may also generate an excessive blandness in messages as their senders try to ensure that the messages do not get flagged: this blandness may itself become a signature; it is also likely that messages between coconspirators will have unusual content." One method to fight fraud is to "pursue a model that describes fraudulent behaviors, or, better, create mechanisms that distinguish

fraudulent from non-fraudulent behaviors (Almeida et al. 2009)." Among other methods, data mining techniques can be used to explore behavioral analysis.

Data Mining

Data mining is a process that analyzes large populations of data and provides useful feedback which can then be more 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 et al. 2009). Almeida et al. (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 et al. 2007).

Data mining can be used to produce models of deceptive practices, fraud, or collusion which assume that word usage changes to reflect factors such as: self-consciousness or guilt about the deception; and simplified content to make consistent repetition easier and to reduce the cognitive burden of generating a false 'story' (Keila et al. 2005). Keila et al. (2005) explain that these models assume that deception leaves a linguistic signature, both because language production is fundamentally a subconscious process, and so affected by emotional states associated with deceiving; and "because the cognitive demands of deception cause performance deficits in other areas." Email communication can be used as data when analyzing an employee's linguistic signature.

Email

Email correspondence in today's business environment is arguably the most common form of electronic evidence (Albrecht *White Paper*), 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). Email is an important vehicle for communication in most companies, both among employees, and between employees and the outside world (Keila et al. 2005) and therefore is extremely affected by any emotional state that the sender is in during composition.

In their research, Keila et al. (2005) analyzed the frequency of first-person pronouns, exclusive words, negative emotion words, and action verbs in emails. Scarcer first-person pronouns like I, me and my, were found to signify an attempted disassociation by the author from their words. Fewer exclusive words like but, without, and except, could suggest the story is fictitious because less of these words represent a less "cognitively complex story." A less cognitively complex, and thus fabricated story is also characterized by a greater occurrence of action verbs. Because of the guilt subconsciously felt by the perpetrator, a deceptive email would also likely contain a higher frequency of negative emotion words. Their approach ranked emails by how likely they were to be deceiving.

Decision Trees

Kirkos et al. (2007) explain that a Decision Tree is a "tree structure, where each node represents a test on an attribute, and each branch represents an outcome of the test." The structure is used to classify a previously unseen object by testing the attribute values of the object against the splitting nodes of the Decision Tree. In their research the selected attribute values were the Debt to Equity ratio, Sales to Total Assets, Sales minus Gross Margin, Earnings Before

Interest and Taxes, Working Capital, Altman's Z score, Total Debt to Total Assets ratio, Net Profit/ Total Assets, Working Capital/ Total Assets and Gross Profit/ Total Assets. They note that the main advantages of Decision Trees are that they provide a meaningful way of representing acquired knowledge and make it easy to extract IF-THEN classification rules. In their research they found the accuracy rate of the Decision Tree model in correctly classifying fraudulent financial statements to be 73.6%.

Neural Networks

Neural Networks is a system that can be used to assist auditors detect fraud. The system consists of numerous neurons or as Kirkos et al. (2007) explain "interconnected processing units". Each connection is associated with a numerical value, called a "weight". These weights are totaled after each neuron receives signals from other connected neurons. The neuron fires if the collective input signal strength exceeds a threshold. The main advantages of Neural Networks are that they "make no assumptions about attributes' independence, they are capable of handling noisy or inconsistent data, and they are a suitable alternative for problems where an algorithmic solution is not applicable." Kirkos et al. (2007) found the accuracy rate of Neural Networks in correctly classifying fraudulent financial statement to be 80%.

Bayesian Belief Networks

Bayesian Belief Networks is a technology that can also be applied to detect fraud. The technology is based on Bayes Law which states that probability measures a degree of belief. Kirkos et al. (2007) explain that Bayesian Belief Networks allow for the representation of dependencies among subsets of attributes. In their research, Kirkos et al. (2007) found Bayesian Belief Networks to be the most accurate in correctly classifying fraudulent financial statements with a rate of 90.3%.

Digital Analysis

Benford's Law

Benford's Law states that in the lists of numbers obtained from natural, real-life data sources, the distribution of the leading digit will follow a long-tail distribution (Hua et al. 2008). Using a mathematical formula, Benford's Law predicts that amounts will start with the digit 1 more often than the digit 9. Despite its limitations, Benford's Law remains one of the most popular data mining techniques for fraud (Albrecht *White Paper*). This is mainly because (1) in most cases, it can be run on data without regard to context, and (2) analysis using Benford's Law does not require extensive training in math, which makes it simple enough to be described to and used by almost anyone (Albrecht *White Paper*). By comparing, for example, sales data, against a Benford's distribution, an auditor can easily see if the number frequency matches that of the Benford's model. If there are anomalies within the data, the auditor can flag these entries for a follow-up investigation.

Zipf's Law

Hua et al. (2008) explain that the basic concept of Zipf's Law is that the frequency of word occurrence in an article furnishes a useful measurement and therefore the management of word significance. This means that a small number of words can categorize a document's content. Zipf's Law differs from Benford's Law in that it can verify diverse attributes other than numeric attributes (See Figure 3.). This allows auditors to filter any potential fraud records or entries, which have abnormal frequency pattern (Hua et al. 2008). Hua et al. (2008) note that the main purpose of Zipf's analyis is to assist auditors for reviewing and identifying any potential fraud records. Figure 4. depicts the process for detecting fraud using Zipf Analysis. In their research, Hua et al. (2008) found that using Zipf's analysis was more effective and efficient than 100% sampling.

Benford's Law	Zipf's Law
They are both derived from Nature Laws	
They can be used to handle disaggregated account level data.	
They both follow the principle of Power Law	
Shows the relationship between digit and frequency.	Shows relationship between rank and frequency.
Numeric attributes are required	No pre-requirements defined for type of attributes.
Applied for fraud detection already	Under review as potential tool for fraud detection

Figure 3. Comparison between Benford's Law and Zipf's Law
Source: Hua et. al. 2008

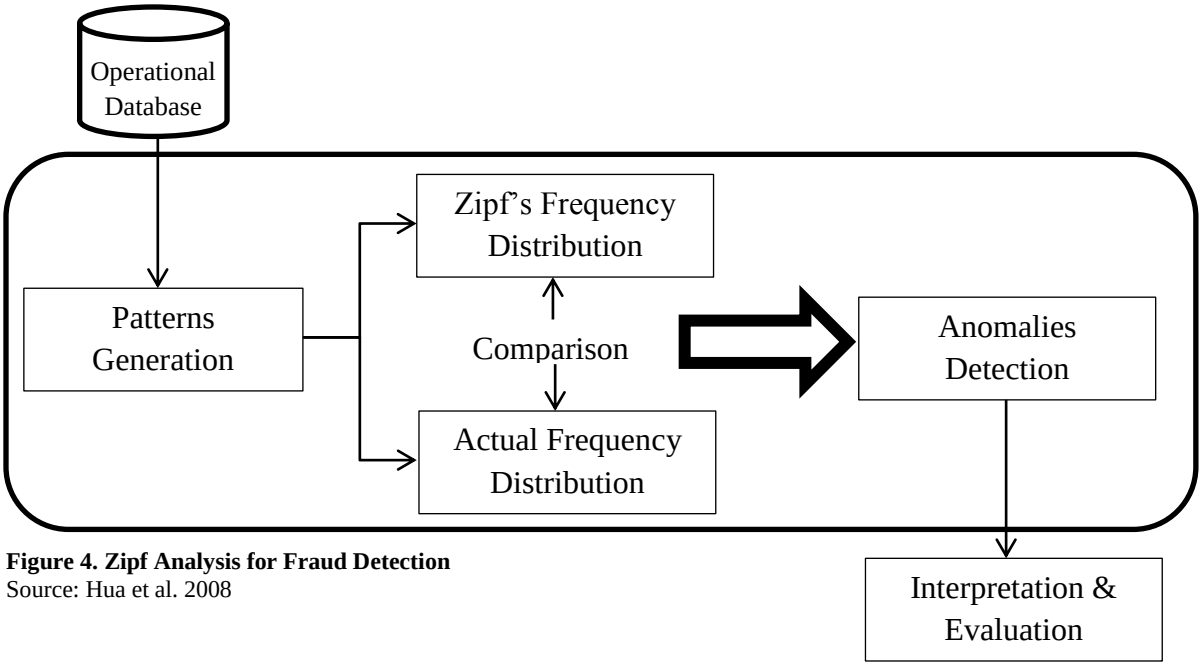

Figure 4. Zipf Analysis for Fraud Detection
Source: Hua et al. 2008

XBRL

XBRL, eXtensible Business Reporting Language, is "a language for the electronic communication of business and financial data which is set to revolutionize business reporting around the world (aicpa.org)." The mandatory filing of XBRL documents for business reporting was phased in starting in 2009 but, organizations who had voluntarily adopted XBRL for their

filings found the cost, time and technical proficiency thresholds to the adoption to be relatively low (Gray et al. 2009). The adoption of XBRL, according to Grey et al., for internal financial data affords opportunity to lower corporate risk, increase efficiency and transparency and better serve stakeholders and the marketplace (Gray et al. 2009).

XBRL increases efficiency and effectiveness because data in this format is retrieved more easily and can be analyzed with greater accuracy (Skillicorn et al. 2007). See Figure 5. for an overview of XBRL structure and format. Because data can be retrieved more easily and with greater accuracy, data analysis for fraud detection and prevention of fraud using data in the form of XBRL is more effective and efficient. Also, Grey et al. (2009) note that there are two important aspects of XBRL (1) its potential to function as a means to exchange data between applications and (2) its map-once-use-many functionality, this is evidenced in that some of the specialized auditing tools, such as ACL and IDEA, are now capable of working directly with XBRL data.

Social Networks

Every organization is built on its relationships between other organizations and the people in the organization themselves. Therefore, it is important to look at the social network of each organization (Almeida et al. 2009). The analysis of social networks within fraudulent organizations and its people can be extremely important when searching for fraud (Almeida et al. 2009). Social network research has been conducted on Usenet data, in which the "goal is to characterize a dynamic online community as well as determine the "authority" of an individual based on posting patterns." (Bekkerman et al. 2004)

By using Conditional Random Fields (CRFs) an auditor can calculate the "conditional probability of values on designated output nodes given values on designated input nodes." CRFs

can be roughly explained as “conditionally-trained hidden Markov models, with additional flexibility to effectively take advantage of complex overlapping features.” (Bekkerman et al. 2004) The system, as Bekkerman et al. (2004) explain, “obtains social links by extracting mentions of people from Web pages and creating a link between the owner of the pages and the extracted person.” In today’s socially booming environment, online (public) communities have voluminous amounts of data that could be used in the auditing profession.

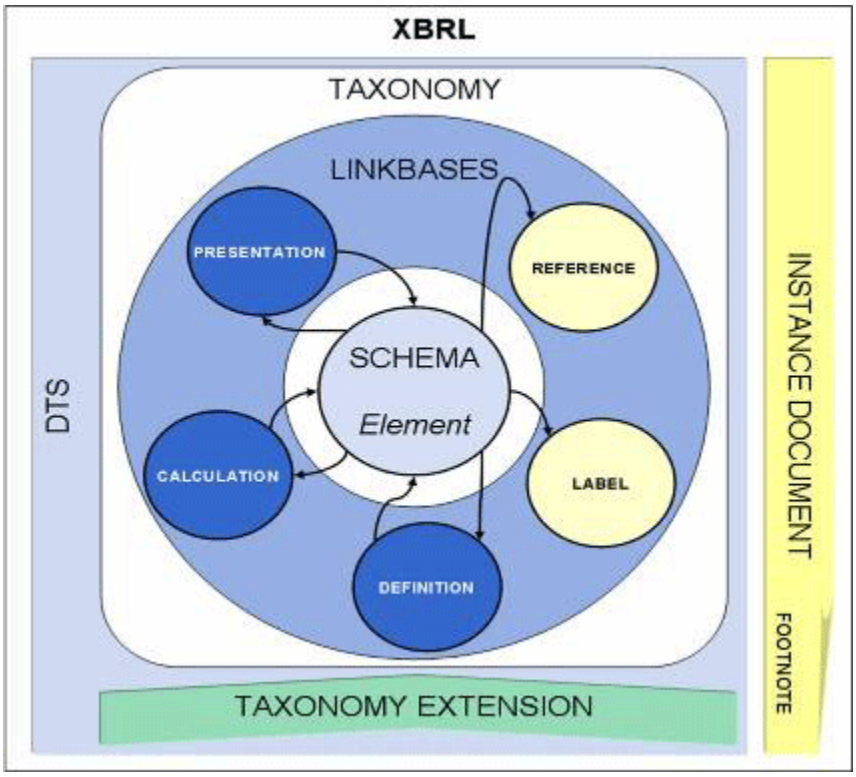

Figure 5. XBRL
Source: ifrs.org

Conclusion

The audit environment today is one of increased responsibility and workload for audit teams, “including enhanced responsibilities for detecting fraud required by SAS No. 99 (AICPA 2002) and internal control attestation now required under Section 404 of the Sarbanes-Oxley

Act." (Curtis et al. 2008) But, if traditional methods of testing controls continue to be used, significant risks may go unnoticed. Bierstaker et al. (2001) note that when dealing with advanced information systems, the auditor may not be able to reduce detection risk to an acceptable level by relying solely on substantive tests. This is why the inclusion of new techniques and up to date resources in an audit is necessary for the efficiency and effectiveness of the final audit, especially for the prevention and detection of fraud.

In the future, the focus of the audit will shift from manual detection to technology-based prevention (Bierstaker et al. 2001). The role of an auditor is changing rapidly, and the use of technology-based audit tools is the only way for the auditor to ensure an effective audit. Technology is essential for auditors to understand the client's business processes and "contend with the paperless audit environment." (Bierstaker et al. 2001)

References

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

Almeida, Miguel Pironet San-Bento. Classification for Fraud Detection with Social Network Analysis. October 2009. *Dissertation, Engenharia Informatica e de Computadores.*

Albrecht, Conan C. Fraud and Forensic Accounting In a Digital Environment. *White Paper for The Institute for Fraud Prevention.*

Albrecht, Conan C., Albrecht, W. Steve, Dunn, J. Gregory. Can Auditors Detect Fraud: A Review of the Research Evidence. 2001. *Journal of Forensic Accounting.* Vol. 2: 1-12.

American Institute of Certified Public Accountants (AICPA). 1988. Consideration of Fraud in a Financial Statement Audit. Statement on Auditing Standards No. 53. NewYork: AICPA

American Institute of Certified Public Accountants (AICPA). 1997. Consideration of Fraud in a Financial Statement Audit. Statement on Auditing Standards No. 82. NewYork: AICPA

American Institute of Certified Public Accountants (AICPA). 2002. Consideration of Fraud in a Financial Statement Audit. Statement on Auditing Standards No. 99. NewYork: AICPA

Bekkerman, R.; Culotta, A.; McCallum, A. 2004. Extracting social networks and contact information from email and the Web. In American Association for Artificial Intelligence.

Bierstaker, James L., Burnaby, Priscilla, Thibodeau, Jay. The impact of information technology on the audit process: an assessment of the state of the art and implications for the future. 2001. *Managerial Auditing Journal.* Vol 16: 159-164.

Byington, J. Ralph, Christensen, Jo Ann. The Computer: An Essential Fraud Detection Tool. 2003. *Wiley Periodicals.*

Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants (CICA/AICPA). 1999. *Continuous Auditing.* Research Report. Toronto, Ontario, Canada: CICA.

Cerullo, M. Virginia, Cerullo, Michael J. *Impact of SAS No. 94 on Computer Audit Techniques.* 2003. Information Systems Audit and Control Association

Coderre, D. 2006. *Global Technology Audit Guide: Continuous Auditing Implications for Assurance, Monitoring, and Risk Assessment*. Montvale, NJ: The Institute of Internal Auditors.

Cullinan, Charles P., Sutton, Steve G. Defrauding the Public Interest: A Critical Examination of Reengineered Audit Processes and the Likelihood of Detecting Fraud. 2002. *Critical Perspectives on Accounting.* Vol 13: 297-310.

Curtis, Mary B., Payne, Elizabeth A. An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. 2008. *International Journal of Accounting Information Systems.* Vol 9: 104-121.

Elliott, Robert K. Twenty-First Century Assurance. 2002. *Auditing: A Journal of Practice & Theory.* Vol 21: No. 1.

Gray, Glen L., Miller, David W. XBRL: Solving real-world problems. 2009. *International Journal of Disclosure and Governance.* Vol 6: 207-223.

Hermanson, D., B. Moran, C. Rossie, and D. Wolfe. 2006. Continuous Monitoring of Transactions to Reduce Fraud, Misuse, and Errors. *Journal of Forensic Accounting* Vol. 7: 17-30.

Hua, Jing-Shiuan, Huang, Shi-Ming, Yang, Luen-Wei, Yen, David C. An investigation of Zipf's Law for fraud detection. 2008. *Decision Support Systems.* Vol 46: 70-83.

Hunton, J., E. Mauldin, P. Wheeler. 2008. Potential Functional and Dysfunctional Effects of Continuous Monitoring. *The Accounting Review* Vol. 86, No. 6: 1551-1569.

Keila, P.S., Skillicorn, D.B. Detecting Unusual Email Communication. 2005. Queen's University School of Computing.

Kirkos, E., Manolopoulos, Y., Spathis, C. Data Mining techniques for the detection of fraudulent financial statements. 2007. *Expert Systems with Applications.* Vol 32: 995-1003.

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

Kuhn, John R. Jr., Sutton, Steve G. Continuous Auditing in ERP System Environments: The Current State and Future Directions. 2010. *Journal of Information Systems.* Vol 24: 91-112.

Nigrini, M., A. Johnson. 2008. Using Key Performance Indicators and Risk Measures in Continous Monitoring. *Journal of Emerging Technologies in Accounting* Vol. 5: 65-80.

Oversight Systems. 2004. *Continuous Transaction Integrity Monitoring for Real-Time Defense Against Fraud and Errors.* Atlanta, GA: Oversight Systems, Inc.

PricewaterhouseCoopers. (PWC) 2006. *State of the Internal Audit Profession Study Continuous Auditing Gains Momentum.* New York, NY: PWC.

Sakagami, M., Shirata, Cindy Y. An Analysis of the "Going Concern Assumption": Text Mining from Japanese Financial Reports. 2008. *Journal of Emerging Technologies in Accounting.* Vol 5: 1-16.

Sarbanes-Oxley Act (SOX). 2002. Public Law No. 107-204. Washington, DC: Government Planning Office.

Shin, Ryan Youngwon. XBRL, Financial Reporting, and Auditing. March 2003.

Skillicorn, D.B., Vats, N. Novel information discovery for intelligence and counterterrorism. *Decision Support Systems*. 2007. Vol 43: 1375-1382.

Wilks, T. Jeffrey, Zimbelman, Mark F. Using Game Theory and Strategic Reasoning Concepts to Prevent and Detect Fraud. 2004. *Accounting Horizons.* Vol 18: 173-184.

Varsarhelyi, M. A., M. Alles, A. Kogan. 2004. Principles of Analytic Monitoring for Continuous Assurance. *Journal of Emerging Technologies in Accounting* Vol. 1: 1-21