Fraud Detection through Routine Use of CAATTs

Sachin Lala, Manish Gupta, and Raj Sharman
School of Management
University at Buffalo, SUNY
Buffalo, NY, USA
{sachinka, mgupta3, rsharman}@buffalo.edu

Abstract— In recent years, fraud has emerged as one of the biggest areas of not just financial loss for most companies, resulting in billions of dollars of loss worldwide, but also of data loss and reputational/brand damage. Overall damage due to fraud can be staggering. In today’s technology-enabled world of business, automated and novel methods of fraud detection are increasingly considered effective countermeasures against the fraud. Due to their expertise and knowledge, IT auditors are being asked to step up to play key role in helping companies fight this battle. Auditors are also progressively relying on technology to assist them with auditing functions. Auditor’s skills and their use of Computer Aided Audit Tools & Techniques (CAATTs), provide unique opportunities for companies to uncover gaps in traditional fraud detection methods. The paper provides insights into existing fraud detection techniques, identifies the gaps and proposes how auditors can leverage CAATTs to fill these gaps, thereby improving overall posture against fraud in companies. The paper will help auditors, fraud analysts and senior management understand how their organization can leverage existing and advancements in CAATTs against fraud.

Keywords— CAATTs; IT Auditing; Security; Forensics; Fraud Detection; IT Automation

I. INTRODUCTION

Auditing for many years had been done only by accountants who verified the controls on finances for organizations. The Big 4 companies as we know started primarily as accounting consultancy firms but have grown to provide many services. Likewise, the process of auditing has also evolved. Auditors are now specialists who are increasingly relying on technology for most of the verifications. In United States, fraud costs organizations hundreds of millions of dollars per year. It is the job of an auditor to detect any illegal activities going on in any organization. Fraud is one of the major issues that are faced by any organization, because it not only causes financial loss but also damages the brand of the company. According to a survey in ACFE’s 2012 Report to the Nations “typical organization loses 5% of its revenues to fraud each year. Applied to the estimated 2011 Gross World Product, this figure translates to a potential projected global fraud loss of more than $3.5 trillion” [1]. According to another survey by ACFE, frauds last a median of 18 months before being reported [1]. These statistics raise the importance of the need to have a thorough assessment of the controls needed to detect and prevent fraud in organizations.

Fraud detection is generally an early warning system for an organization. It comes into picture when a preventive control of an organization has failed [5]. The primary purpose of fraud detection is to identify fraud as quickly as possible and minimize the losses associated with it. Fraud detection not only helps in preventing financial losses but also in improving shareholder confidence and market value. Apart from this, it can also help in refining organization controls and identify dishonest employees [2]. Fraud detection alarms must be in place all the time to give a signal on the failure of fraud prevention controls [5].

In case of a fraud, it is very important that it is identified as quickly as possible. Currently, fraud is detected using various techniques like data mining, statistical analysis and business intelligence. The techniques currently in place are pretty advanced but fraudsters are already adapting to the new technologies. Apart from this, it is a difficult task to obtain all the data required for fraud detection. In some cases, the data may not be revealed due to the confidential nature of data while in some cases it may not be technically possible for a company to provide the required data. Hence, to gain an edge over fraudsters, it is important that detection software also keep evolving. The necessity to tackle fraudsters is one of the reasons why audit specific software was needed and this led to the development and innovations of CAATTs (Computer Aided Audit Tools & Techniques). Audit standards now encourage the use of CAATTs for auditing. E.g. International Standards for the Professional Practice of Internal Auditing (Standards), Standard 1220.A2 – Due Professional Care states that “In exercising due professional care the internal auditor should consider the use of computer-aided audit tools and other data analysis” [46]. Apart from this Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) also has certain guidelines for auditors which allow the use of CAATTs for auditing [32], [33].

The contributions of the paper are two-fold. First it shows gaps in traditional fraud detection methods that call for novel approaches and leverage existing investments in auditing tools and second it provides insights into how CAATTs and auditors can help organization’s anti-fraud efforts and second. The paper is organized as follows: Section II provides background and preliminaries on IT auditing, CAATTs and fraud detection. Section III talks about challenges and gaps in traditional fraud detection techniques. Section IV discusses the approaches that leverage CAATTs to bridge the gaps and provide opportunities for effective fraud detection. Section V presents a brief case to provide an extended example on how CAATT benefits anti-
fraud initiatives. Lastly, in section VI the paper provides conclusion and directions for future research.

II. BACKGROUND / PRELIMINARIES

A. Use of Technology in Auditing

The need for the use of IT for Auditing has increased in the last few decades. There are a couple of reasons – Increase in use of electronic documents large firms developing computerized decision aids to assist themselves in decision making, customer relationship management and analytical procedures [18], [19], [20] and impact of IT on the behavior and attitude of individuals [4]. There are several benefits as well of IT auditing. IT can reduce the time auditors spend performing computational tasks and improve the quality of audit by structural audit decision process [21], [4]. IT also appears to increase audit quality and productivity through audit automation, eliminating certain audit procedures, enhancing information and knowledge-sharing capabilities [21], [4]. Recent standards also codify the increase in use of technology for auditing [29], [30], [31], [32]. IT auditing consist of all the things designed to enhance the capacity of the auditor to perform an audit task [4], [23].

The manual auditing has become too time consuming in light of amount of data available for analysis. With the advancement in technology, organizations have started relying more on computers to store and transfer their data. The advancement in technology has also lead to increase in threats. Hackers, viruses, DOS attacks etc. can all affect the confidentiality, integrity and availability of critical processes and data of the organization and can cause huge losses. As the organization grows, the auditor needs to depart from the traditional approach and move towards new technology for auditing. “The pervasive nature of information technology, the favorable economic and functional versatility of modern computing technology and the globally open and competitive market forces that drive the rate of technological evolution are together creating an era of profound change in the market place for audit automation” [24], [25], [26].

B. Fraud Detection

ACFE defines fraud as “the use of one’s occupation for personal enrichment through the deliberate misuse or application of the employing organization’s resources or assets”. Companies and individuals lose billions of dollars every year to various types of fraud [44], [53], [54], [55]. The proceedings from these frauds helps fund organized crime, international trafficking, and even cross-border terrorist financing [55]. There is mounting pressure on companies to automate fraud detection [51], [52]. Fraud presents has emerged as a serious problem in many different areas such as health care [45], banking [47], insurance [48], and networking [49], tax [39] and customs [40]. There have been numerous studies to investigate fraud detection. For example, data mining has been proposed as an effective method [37], [40], [41], [42], [43] and monitoring devices have been proposed for corporate fraud [56], [57]. Automated fraud detection has been researched in specific areas such as spam [54] and network intrusion [50]. At the same time, there have been studies that have suggested challenges and criticism to existing methods [5], [36], [37], [38].

C. Auditor’s Involvement in Fraud Detection

One of the most difficult challenges faced by organizations is detection of fraudulent activities. Fraud can be of many types and in some cases, fraudsters can get away by committing the crime which cannot be detected easily. Fraud is an illegal activity that is hidden and used for personal gains. Without the use of data analysis software, auditors will not be as efficient in detecting the crime. Fraud can be either to benefit the organization or for the personal benefit of the employee. In either cases, detecting fraud is not an easy task. As per audit standards, auditors are required to gather as much fraud risks as possible while verifying controls a system. Several scandals in the last few decades have increased the need of auditors in the detection of fraud.

There is a need for IT auditors should try their best to innovate new tools and technologies for the detection of fraud in an organization. Every organization has certain controls and measures in place to secure their information and also prevent fraudulent activities. Although, it is management’s responsibility to design the controls, it is the auditor’s responsibility to ensure that proper controls are in place that can detect true nature of the fraud and report it also. Auditor needs to be actively involved in detection of fraud. IT Auditors have the necessary knowledge and expertise about the security controls in place. Hence, auditors are in a very good position to check the breach of controls and gather the evidence needed to detect the fraud. Fraudsters keep adapting to the fraud detection techniques and hence, auditors also need to adapt to latest technologies to detect fraud. According to a The 2013 Federal Reserve Payments Study, Total number of credit card transactions in the U.S. in 2012 was 26.2 billion [13]. Processing data sets with such huge amount of data needs much more than statistical models for fraud detection. Hence, CAATTs have the potential to become an integral part of the auditing process.

D. CAATTs

CAATTs are computer tools used by external or internal auditors as a part of the audit procedures to process significant data contained in organizations information systems [3]. Research has shown that the types of CAATTs can be classified to include the following groups: electronic documents, fraud prevention and detection, information retrieval and analysis, network security, continuous monitoring, audit reporting, database of audit history, computer based training, electronic commerce and internet security [3]. Computer Assisted Audit Techniques and Tools (CAATTs) are not used by businesses as an ad-on, rather they have become an integral part of many audit methodologies [22], [34]. Use of CAATTs by auditors is dependent on company’s size and the industry in which it operates [35]. An estimate suggests that more than 50% of internal auditors in United Kingdom use CAATTs, but spend less than 10% of their time on them. But this improves for 67% of the internal auditors increase the use of CAATTs up to 50% with time [3].
Using CAATTs for auditing is not mandatory but use of CAATTs can assist auditors in many ways. With the use of CAATTs, the auditor can concentrate on the core process of auditing and let CAATTs complete the ad-on tasks. The amount of time saved because of CAATTs is huge and this directly results in cost saved for the organizations. For few organizations, CAATTs have been adopted for the core part of audit process as well. However, CAATTs can be considered only as tools to assist the auditors in calculations and doing faster tasks. CAATTs cannot be a replacement for the auditors. Auditors are still required to verify the results obtained from CAATTs and use their knowledge and experience to confirm the results.

The main purpose of using CAATTs is that it improves the ability of auditors to interact with the data, converting facts and figures into useful information that can help provide recommendations and result in subsequent actions. The interactive nature of CAATTs allows auditors to discover the meaning behind the numbers and develop a better understanding of both the data and the reality it supports. The software makes analysis easy to formulate and perform. Hypotheses can be formulated, tested, and revised as necessary, based on the results of initial interactive analyses.

CAATTs also provide auditors with the ability to quickly and efficiently extract information from several databases with disparate database management systems, and identify underlying patterns or relationships in the data [12]. According to an article on ISACA, The software used as CAATTs can be classified into below categories. - Data Analysis Software, Network Security evaluation software OS and DBMS security evaluation software, Software and code testing tools [11].

III. GAPS AND CHALLENGES IN THE TRADITIONAL FRAUD DETECTION PROCESS

According to a recent study that analyzed auditors deficiencies in the US SEC Fraud Investigations between 1998 and 2010 a total of 87 Fraud Detection failures by auditors were found. Table 1 shows some of the audit deficiencies which caused fraud [7]:

The frauds have resulted in multiple regulations that organizations are mandated to comply with. Sarbanes-Oxley act is one of the regulations which have helped prevent many cases of fraud. As per AICPA section AU 316.13, auditors need to keep questioning and have a thorough assessment of audit evidences. There can also be bias created due to the relationship between the client and the auditor. Unconscious human nature may build certain associations which may lead to ignorance of certain key evidences [8]. Even with the current regulations and strict measures taken by auditors, there are certain deficiencies in the audit process and the controls which result in fraud. Increasingly, auditors are how relying on CAATTs to detect fraud.

A. Fraud Detection Using CAATTs

CAATTs can definitely assist in fraud detection, but even more important is the auditor’s ability to recognize

![Fraud Detection Using CAATTs](image_url)
opportunities. CAATTs have the ability to improve the range and quality of audit and fraud investigation results. CAATTs are interactive and give a lot of flexibility to the auditors to perform the desired operations. With the emergence of CAATTs, the auditors need to move from the traditional approach. Using, data analysis software, auditors can get new set of tools to recognize opportunities of detecting fraud. Figure 1 shows the process of fraud detection after a fraud is reported. An auditor is assigned to the task. The auditor creates a formal fraud investigation plan. The fraud plan should have clear definition of why the fraud investigation is taking place, when it will take place, where it will take place and how it will take place. The plan also contains details of the CAATTs software to be used for the fraud detection. The auditor then needs to source the data. To source the data, the auditor will meet the owner of the data, request the data and when the request is approved, the auditor will use CAATTs to extract the data. The auditor can use several techniques to extract the data – the auditor can obtain logical access to the systems, run ad-hoc queries or gain direct access to the client data. The next step in fraud detection would be to understand data. CAATTs can help auditors in understanding the data. The client data can be on various platforms and CAATTs can help convert the data in a common format that can be understood by the auditor. E.g., Data on mainframe systems would be in EBCDIC format and CAATTs can help it convert to a format that can be read in a normal text file. While extracting data, auditors should also take care that the right fields are extracted in the right manner so that the integrity of the data is not affected. The extracted data can then be summarized and stratified to examine the possible range of fraud. To detect fraud, auditors may have to extract data from various sources and then merge it. Hence, joining the data from various sources is important. The auditor can then use the trend or pattern analysis to identify the fraud occurred and the source of fraud. In many cases, the auditor may have to use multiple ways of pattern analysis to detect a fraud and its source. In the end, the auditor will draft the results, verify it and send it to the organization in a report format [6].

<table>
<thead>
<tr>
<th>Problem Area</th>
<th>% (Number of Cases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to gather all competent audit evidences</td>
<td>73% (59)</td>
</tr>
<tr>
<td>Unable to take due professional care needed for the audit</td>
<td>67% (54)</td>
</tr>
<tr>
<td>Failure to obtain adequate evidence related to management representations</td>
<td>54% (44)</td>
</tr>
<tr>
<td>Wrong interpretation and application of requirements of GAAP</td>
<td>37% (30)</td>
</tr>
<tr>
<td>Inadequate consideration of fraud risks</td>
<td>33% (27)</td>
</tr>
<tr>
<td>Failure to adequately address audit risk and materiality</td>
<td>21% (17)</td>
</tr>
<tr>
<td>Failure to prepare and maintain audit documentation</td>
<td>20% (16)</td>
</tr>
<tr>
<td>Failure to perform all audit procedures</td>
<td>15% (12)</td>
</tr>
<tr>
<td>Failure to evaluate all internal controls</td>
<td>14% (11)</td>
</tr>
</tbody>
</table>

Auditors can create templates for patterns of fraud and feed these to CAATTs. The CAATTs can thus help detect fraud based on such patterns. This can be a very useful initial scanning approach which can help identify fraud at early stages and also save auditor’s time. The CAATTs can also use these patterns for continuous monitoring of systems. This will help enable auditors catch a fraudulent activity before it becomes critical [14].

Below are some of the techniques to detect fraud using CAATTs [15]:
- Calculation of statistical parameters – calculating average, standard deviation to find fraudsters outside the required calculation limit
- Pattern classification – to find trends or patterns in data and detect an unusual pattern
- Stratification – to identify unusual number of entries
- Benford’s Law – to identify unexpected occurrences of digits or combination of digits
- Joining different diverse sources – to identify invalid columns which match in a dataset but should not be present there
- Duplicate testing – to identify duplicate transactions.
- Gap testing – to identify missing values in sequential data
- Validating entry dates or time – to identify transactions during suspicious date or time

The discussion in the section III provides examples that have caused huge losses to the organizations and also raised questions on the resources available with the auditors to take due care while gathering evidences and maintaining audit documentation. This is an area where the use of CAATTs can benefit the auditors and help detect fraud. A study of the literature review shows that, The Triangle of Fraud Action is a term which is used sometimes when there is a mention of fraud detection [17]. The Triangle of Fraud action gives a model to detect fraud that cannot be otherwise identified and also preserve and maintain the evidence related to fraud. As we can see in the Table 1, maximum (73%) number of fraud take place because the auditor is unable to gather enough evidences of fraud. In around 54% of the cases, the auditor is unable to obtain adequate evidence related to management representations, in 20 % of the cases, the auditor fails to prepare and maintain audit documentation and in 14% of the cases, the auditor fails to adequately evaluate all internal controls [17]. All the above cases could have been prevented with the efficient use of CAATTs.

The Triangle of Fraud Action, if incorporated in the use of CAATTs can help reduce a major percentage of fraud. The elements of the Triangle of Fraud Action give the details of the actions that must be performed to prevent fraud. The three elements of the Triangle are act, concealment and conversion. [17], [27], [28]. The Triangle of Fraud Action can not only prevent fraud but also make it difficult for the fraudster to deny that he had committed the fraud. This in turn, helps the auditors to confirm their decisions and gather enough evidences against the fraudsters.
Auditors need to impart the intelligence in CAATTs to detect and prove the fraud based on the three elements of the Triangle of Fraud Action. Figure 2 shows how the capabilities of CAATTs interfaces with the elements of the triangle of fraud action. The first element, The Act is the most common techniques of fraudulent reporting in an organizations financial statements. E.g., Overstatement of Assets, misrepresentation of Assets/Liabilities etc. These are done through the misleading entries in the financial reports and there are certain types of models which possibly can be successful in covering the fraud [17]. The auditors should ensure that the CAATTs are enabled to catch such type of patterns which can escape manual auditing and also are difficult to prove.

The second element of the Triangle of Fraud Action, concealment is the way in which a fraud can be hidden so that it cannot be detected easily. To prevent concealment of fraud, CAATTs need to be developed in such a way that it understands the methods used to conceal a fraud. For e.g. Inadequate disclosure of all agreements, inappropriate general ledger entries etc. If CAATTs can be modelled in such a way that it can catch the complex techniques used to hide the data, a major percentage of the auditors task can be made easy.

The third element of the Triangle of Fraud Action is Conversion. It involves the conversion of fraudulent reporting into personal gains [17]. E.g., wrongly stating the receipt of bonus based on overstated earnings. Such methods of conversion of a fraud into profit can be identified and caught through the use of computer technology. If intelligence to catch the patterns and models for the three elements of the Triangle can be imparted in CAATTs, a significant percentage of fraud can be reduced.

IV. LIMITATIONS & CHALLENGES ASSOCIATED WITH CAATTs

While CAATTs are useful in many cases, there are also certain challenges associated with use of CAATTs. Many decisions made by the auditors are based on their experience and knowledge of auditing. CAATTs can perform tasks in a much faster time but there is no decision making ability in any of the CAATTs. Such cases arise in case of regulations or compliance controls, where there is a difficult judgement call to be made and the auditor cannot depend on CAATTs for it. The compatibility of CAATTs is another challenge faced by the auditors. All CAATTs may not be compatible with the IT infrastructure in the organization. Certain CAATTs may need additional software or hardware to get executed on time. Even if the CAATTs are compatible, performance of CAATTs can become an issue in some cases. CAATTs are based on statistical analysis and automated procedures. There is a possibility that white collar crimes may get filtered out of the data by CAATTs as the software will not detect any unusual pattern in it. Using CAATTs for auditing always requires production data access by auditors. There is always a fear of accessing the data in an unauthorized manner or the CAATTs affecting the performance of the system which stores the production data. The organization may not give complete access to the auditors and the fraud may remain undetected.

V. CASE STUDY – LET CAATTs LOOSE ON FRAUDSTERS

Enron was an energy company, owning electric-power production facilities and natural gas pipelines. Since 1990, Enron moved into the business of trading energy vehicles, future electric power and natural gas contracts, water rights, wind power systems, broadband transmission systems, insurance and other products [9]. Enron expanded into several areas like developing a power plant and a pipeline. This expansion required large amount of investments. By that time, Enron already had a lot of debt and getting future funds would have affected Enron’s credit rating. Hence, Enron began creating “Special Purpose Entities” or SPE’s. These companies were used to hide Enron’s debts from its financial statements. The corporation followed this policy which meant that it was rated high by rating agencies and Wall Street analysts [10].
Accounting firm, Arthur Anderson were involved in the internal and external auditing process for Enron. In 2001, Arthur Anderson reviewed one of Enron’s SPE’s and concluded that its accounting had been incorrect. Enron announced that it was taking $544m after-tax charge against earnings related to transactions with LJMZ Co Investment, one of the SPE’s. Enron also found that in certain transactions, it had exchanged its shares for notes receivable and incorrectly recorded the transactions as an equity growth of $1b. Proper accounting would have shown that Enron’s shareholder equity was reduced by $1.2b. Enron stock collapsed after this and the company filed for bankruptcy in December 2001 [9]. Enron’s executives, investment banking partners and the company’s accounting firm, Arthur Anderson were held responsible for the illegal practices. (Lucian & Cristina)

In such kind of frauds, continuous auditing can be used for continuous monitoring and detection of fraud. Continuous Auditing is one of the techniques used as a part of CAATTs to evaluate controls and detect fraud as it happens. Continuous auditing through CAATTs if effectively used, can provided an assurance of processes that may not be present in the financial report of the organizations. CAATTs rely heavily on the analysis across different processes and risk attributes. CAATTs used for continuous auditing can produce audit results simultaneously with relevant events. CAATTs can also go into more granular level and expand the scope of the audit to verify extraordinary transactions as well. In a continuous audit, CAATTs continuously monitor transactions and compare them to expected results. Any discrepancies in the actual and expected results trigger alarms that the auditors and company’s management cannot ignore.

CAATTs if used in a proper manner, can be used to reduce the time taken to detect such frauds. For eg. CAATTs could have been used to continuously monitor Enron’s processes and it would have triggered an alarm when many ratio’s of Enron’s SPE’s would not be consistent with those of its competitors. Also, the value of Enron’s components would not have added to match the totals and triggered alarms to look for undisclosed entities [16]. Continuous monitoring and detecting can assist in bringing such unreported partnerships and brought the fraud into light much earlier. The data flows would question the huge nonrepetitive data flows between Enron and its SPEs. CAATTs could then report these issues to the higher authorities and issue a warning that cannot be ignored[16].

VI. CONCLUSION AND FUTURE RESEARCH

The paper presented how fraud detection has gained momentum in industry and in academia due to the emergence of newer fraud techniques and capabilities. To thwart fraud attempts by early detection, it has been unanimous in choice that automation is the way to go. The costs presented by new fraud detection techniques hampers development of new tools and software. In light of this, auditors who are skilled and knowledgeable in the areas of fraud can be equipped with CAATTs that they can also leverage for fraud detection. The paper surveyed the challenges and gaps in current fraud detection methods and how specific attributes of automated IT auditing can benefit the practice. The paper presented characteristics of CAATTs that can be used for fraud detection by auditors as part of their routine job functions. This proactive and incremental approach to fraud detection is less drastic and expensive but immensely effective. As next steps in the research, a detailed survey of extant CAATTs and their operational characteristics could be conducted to identify the areas where they can be improved and more effectively deal with fraud detection. Also, a section on managerial and practical implications can also be added for readers benefit. Also, a conceptual framework can be developed for providing a path for companies to efficiently capitalize their investments in CAATTs and auditors for also detecting fraud. Use of Routine Activity Theory can also be ensued to demonstrate how auditor’s defined functions and use of CAATTs can provide benefits in the area of fraud detection. In other words, auditors will continue to do their function as auditor but by using incremental features in CAATTs they may provide insights into frauds as part of their routine activities.

REFERENCES


