An Overview of Research on Auditor’s Responsibility to Detect Fraud on Financial Statements

Dr. Mohamed S. M. Salem
Accounting, Finance and Economics Department, University of Sharjah, United Arab Emirates (UAE)

ABSTRACT

Researchers and practitioners have made many attempts to identify fraud indicators and to build fraud prediction procedures. Fraud is a beg subject and causes tremendous loss to the business world and creates morale problems in the workplace. It represents a critical issue for the accounting profession, in devolved and non-developed countries. Numerous surveys in the 1980s have served to underline the significance and extent of fraudulent activities within profit and non-profit organisations. Then, the need to fight fraud has exerted strong pressure for auditors to assume this role. In this respect, the auditor’s role to prevent and detect fraud is a very important part of his/her job because of the use of advanced and complex computer systems. As a consequence, this paper is concerned about fraud, based on the primary responsibility for prevention and/or detection of fraud rests upon management to develop adequate accounting systems with appropriate internal controls. This paper discusses the various facets of financial fraud, what constitutes auditors’ breach of duties to their clients and reporting of fraud. Overall, this paper highlights certain weaknesses present in prior fraud detection studies. These studies reveal that because of the use of more advanced technology, the amount of fraud that is detected appears to have declined. In addition to this, auditors have limited legal expertise and do not have the training needed to identify all illegal activities.

Keywords: Fraud Detection, Management Fraud, Fraud and Computer.

INTRODUCTION

Fraud has become very complicated in this era of technology, and increasingly difficult to detect, especially when it is collusive in nature and committed by top management who are capable of concealing it. In this respect, auditors have argued that the detection of fraud should not be their responsibility (Alleyne and Howard, 2005). Consequently, the term fraud in prior auditing standards referred to irregularity which incorporated fraudulent financial reporting as well as employee theft and embezzlement, we limit our focus to management fraud or fraudulent financial reporting, which relates primarily to management’s intentional misrepresentation in financial statements (Guan, et al., 2008). The current study looks slightly at financial statement fraud by managers and/or employees who have sufficient authority to override an organisation’s internal controls. Generally, such fraud involves deliberate distortion of accounting records, falsification of transactions, or misapplication of accounting principles. Regardless of how the fraud is manifested, it is typically difficult for auditors to discover since the perpetrators take steps to deliberately conceal the resulting irregularities. Given the difficulty that auditors face in detecting financial statement fraud, coupled with their increasing responsibility to detect it, there is a definite need to develop audit procedures or strategies more specifically focused on fraud detection (Knapp and Knapp, 2001; Guan, et al., 2008).

Over the last two decades, there have been developments concerning fraud which some have seen as marking significant extension to audit responsibilities. The business community, especially the accounting profession, has become increasingly concerned about the rise in management fraud. Recent internal reports suggest that employee fraud is pervasive, plaguing both large and small organisation alike. According to the 1996 report in the Nation on Occupation Fraud and Abuse, fraud and abuse cost US organisations more than $3.9 billion annually (Hillison, 1999). Furthermore, the Association of Certified Fraud Examiners (ACFE) in their survey for 2008 estimated that US companies lose 7 percent of their annual income to fraud, resulting in approximately $995 billion in losses (ACFE, 2008). The ACFE also estimated that the typical company loses 5 percent of their annual revenue to fraud which the
ACFE estimate that this 5 percent figure would translate to approximately $2.9 trillion as applied to the estimated 2009 gross world product (Crawford and Weirich, 2011). For instance, almost daily one can read about organisations that have been exploited in both the private and public sectors resulting in embarrassing, fraudulent schemes and the loss of assets (Alleyne, et al., 2010). Not only has the incidence of fraud increased, but the dollar amounts of fraud and the number of companies being victimized have also increased (Humphrey, 1993; Hemraj, 2004). Because of this situation, a number of individuals and groups, shareholders, corporate audit committees, and the Securities and Exchange Commission (SEC) are feeling the pressure of the responsibility to detect an increasingly sophisticated ‘fraud industry’ (Guan, et al., 2008). Even though auditors have been willing to accept the increased responsibility to uncover fraud, their basic training for this task (Alleyne, 2010; ACFE, 2008) needed to be developed.

Numerous surveys in the 1980s have served to underline the significance and extent of fraudulent activities in the corporate sector (APC, 1988; Humphrey and Turley, 1993). In this respect, the auditor has a duty to search for fraud and is expected to detect fraud by the exercise of professional skill and care (Rittenberg and Schwieger, 2005). However, the auditor's role to uncover material fraud is a given. Interpreting and fulfilling this role is less obvious and more complex. As Hemraj (2004) reported that is because fraud occurs rarely, or perhaps it is because the majority of people are honest or that the existing internal accounting controls are effective in promoting an honest climate. As a result, auditors may not always be aware of the potential for fraud or they simply fail to recognize the signals when fraud is present. In order to fulfill his role more fully, the auditor must understand the nature of fraud and its consequence on planning and conducting his audit (Guan, et al., 2008; Ernst and Young, 2002).

According to Helsby and Kaizer (2003) and Venter (2007), in an economic crime survey conducted in Europe during 2001, in most cases fraud in enterprises is discovered by chance. They also mention that although enterprises appear to have control systems in place, in many cases, these are ineffective, primarily due to the fact that management either overlooks controls, or colludes in circumventing them. Most frauds involved an employee or manager of the victims’ organization (Seetharaman, et al., 2004). In this respect, auditors must always keep in mind that fraud is committed by top management may be more prevalent and harder to detect because an employee may be less likely to object if he/she is ordered to make false entries, and less likely to report his/her knowledge that the other person is doing so. Also, Stockholders, audit committees, and top management are more insistent about being informed of fraud and more likely to fault the auditor if it is not found and reported (Rittenberg and Schwieger, 2005). During the last twenty years, the growing concern over fraud leads to a false perception by the financial statement users of the auditor’s role as extending to the detection of all sorts of fraud (Skousen, et al., 2009). This paper is mainly concerned with fraud, based on the author’s point views and sample of prior researches’ results which are possible to detect organisation scandals by tackling fraud.

This paper seeks to answer questions relevant to fraud, fraud detection, and fraud and technology associated with fraud prevention in computers. These key questions are: first, what is a fraud and what can be done about it? Second, what are persons’ motivations and earnings management to commit a fraud? Third, who in an organisation is in the best position to detect and prevent fraud? And, fourth, in what sense does management and/or auditor can prevent fraud and how fraud can be prevented in computers? In this respect the paper will answer and analyse these questions in the context of management and auditor responsibility to detect fraud. Further, the present paper contributes to key aspects of fraud that auditor should look to improve the internal control systems and build an audit program which follows generally accepted auditing standards. It contributes to the knowledge and understanding of the nature of fraud and the auditor’s responsibility to detect material fraud. The paper also identifies the implications of frauds and errors which are material to the financial statement and may not be detected due to an oversight, but without negligence on the part of the auditors or management. For example, UK organisations which do not provide enough information to evaluate fully management efficiency, effectiveness and performance which are needed for fraud detection.

The remainder of the paper proceeds as follows: Section 2 looks at the selective review of the literature and fraud detection concerning brief historical background, auditor’s role for uncovering fraud, key characteristics of fraud perpetrators and motivations, and common symptoms of acts of fraud. The third section looks at how fraud can be prevented in computer technology. The next section identifies methods of computer security to reduce fraud. This followed by the fifth section related to study’s conclusions and contributions.
SELECTIVE REVIEW OF THE LITERATURE AND FRAUD DETECTION

Brief Historical Background

Fraud causes tremendous losses to the business world and creates morale problems in the workplace. These losses are serious problems to organisations that need to be managed, controlled and monitored. Technology, the criminal and law enforcement are continuously leapfrogging each other, as the race continues to build better tools, commit bigger crimes and develop more effective law enforcement (Rittenberg and Schwieger, 2005). Fraud detection is an examination of the facts to identify the indicators of fraud. Reviewing and improving the internal control system is the primary defence against fraud and abuse. This study showed that a strong system of internal control is the most effective way of fraud prevention. Hence, the aim of this effort is to raise the level of security awareness for organisations in order to plan and facilitate a concerted effort to battle fraud, as prevention is better than cure (Uzun, et al., 2004).

The literature in the field on fraud detection has evolved over the years. Some authors have acknowledged that there are limitations in the way individual auditors make fraud judgments (Wilks and Zimbelman, 2004) and ultimately find it difficult to identify fraud (Kapardis, 2010; Carpenter, 2007; Knapp and Knapp, 2001; Pincus, 1989). However, during the period of 1980s, there have been developments concerning fraud which some have seen as marking significant extensions to auditor responsibilities (Humphrey, 1993). Although the auditor’s responsibility for detecting fraud has not changed from Statements Auditing Standards (SAS) No. 82, the amended standard provides more guidance on how the auditor should plan and perform the audit (including the use of analytical procedures) to identify the risks of material misstatements arising from errors or fraud (Albrecht, et al., 2009; Arens, et al., 2008).

Consequently, the Auditing Standards Board (ASB) in 1998 issued statement on auditing standards imposed greater responsibility on auditors to detect financial statement fraud. The ASB formed a task to reconsider auditors' responsibility for the detection of fraud and provides operational guidance to practitioners (Knapp and Knapp, 2001). Moreover, most accounting practitioners realize and acknowledge that auditors are often not positioned to detect the occurrence of fraud. Auditors lack the continuous presence necessary for the establishment and implementation of fraud prevention and deterrence programs. Unlike other crimes which may be witnessed, fraud, by its very nature, typically entails concealment by its perpetrators.

In recent years, more attention has focused on management fraud and on the failure of auditors to detect and report the fraud. As highlighted previously in this study, the literature provides ample evidence of fraudulent activities especially in the USA. Consequently, the decade of the 1990s witnessed a substantial increase in fraud. According to the UK Audit Commission, frauds have increased by approximately 38 percent since 1990 (Owusu-Ansah, et al., 2002). This increase in fraud has led to a corresponding increase in the dollar value associated with fraud. For example, a study by the ACFE in the USA revealed that over a ten-year period the cost associated with 2,608 reported fraud cases totaled US$15 billion (Owusu-Ansah, et al., 2002). Such fraud has caused a loss of public confidence in audited financial statements, and has mandated the need to reconsider the procedures performed to uncover fraud in current and future financial statement audits (Alleyne, et al, 2010).

The role of the auditor has not been well defined from inception. In the nineteenth century, auditors claimed fraud detection as an audit objective (Alleyne and Howard, 2005). It has been also stated by Bishop (2004) that the auditor’s duty is to report to shareholders all dishonest acts which had occurred and which affected the propriety of the contents of the financial statements. However, the learned judge also argued that the auditor could not be expected to uncover all fraud committed within the company, since the auditor was not an insurer or guarantor, but was expected to conduct the audit with reasonable skill and care in the circumstances. In this regard, Hillison, et al., (1999) indicated that the primary roles of preventing and detecting fraud within organisations lie with the management. In practice, the auditor is normally concerned with a suspected rather than proven fraud or irregularity. Nevertheless, the auditor should be able to detect all material fraud (Hassink, et al., 2010). Furthermore, fraud, in whatever nature and guise, has to be detected first, since detected is an important prerequisite of rooting out any sort of. On their own, auditors are not necessarily the most suitable group to perform the task of fraud detection. The company, by instituting appropriate fraud prevention measures within its organisation, can detect and prevention non-management fraud (Hemraj, 2004). This is because...
management fraud involves circumventing internal control procedure and often escapes detection until a company has suffered irreparable damage (Carmichael, 2004). Management fraud is also essentially fraudulent financial reporting or misapplication of accounting principles (Albrecht et al., 2010). An example would be an overstatement of ending inventory on the balance sheet to show more inventory on hand than is actually there, thus intentionally overstating assets and revenues. As a result of fraudulent activities occurring in Enron, WorldCom and other companies, the Sarbanes-Oxley Act of 2002 has required that internal controls be reviewed and that adequate fraud detection and prevention systems be implemented (Alleyne et al., 2010; Albrecht et al., 2009). This suggests that fraud detection must be high on the auditors’ agenda.

Auditor’s Role for Uncovering Fraud

The area of fraud detection is particularly important from the investor’s perspective. Generally, all investors want to protect their investments and want to be reassured that the assets of the company are correctly stated and safeguarded (Alleyne, 2005). It is also important that auditors are even more vigilant in the execution of their responsibilities by ensuring that due diligence and care is at the forefront of their agenda so that fraud can be detected and exposed. This is critically important, if auditors are to protect and preserve their professional reputation and integrity and avoid legal costs (Makkawi and Schick, 2003).

Fraud may occur because the responsibility for its prevention is not a normally assigned task, because dishonesty is accepted as inevitable, known cases go unpunished, and the disease spreads; because security is thought too expensive or covered by fidelity bonds. It may also persist when its prevention is not taken seriously and when dishonesty is accepted as something that cannot be avoided. Fraud exists when one or more of the following conditions exist: 1) misappropriation of assets, 2) overstatement of assets or understatement of liabilities to present more favorable financial position and/or result of operation, 3) theft of assets through transactions with branches or subsidiaries of the parent company, and 4) lack of disclosure of significant information (Elder, et al., 2010).

Moreover, the role of the auditor has not been well defined from inception. In the nineteenth century, auditors claimed fraud detection as an audit objective. Porter (1997) indicated that it was the auditor’s responsibility to report to shareholders all dishonest acts which had occurred and which affected the propriety of the contents of the financial statements. However, the learned judge also argued that the auditor could not be expected to uncover all fraud committed within the company, since the auditor was not an insurer or guarantor, but was expected to conduct the audit with reasonable skill and care in the circumstances (Carmichael, 2004). As indicated by Vanasco (1998) during the 1930s, it became generally recognised that the principal audit objective was the verification of accounts. The profession took the position that fraud detection was management’s responsibility since management had a responsibility to implement appropriate internal control systems to prevent fraud in their organisations. This was as a result of the increase in size and volume of companies’ transactions that made it virtually impossible for the auditor to examine all transactions (Porter, 1997). Auditors used sampling and testing procedures, which offered only reasonable assurance of the contents of financial statements. In addition, auditors were unable to uncover fraud that involved unrecorded transactions, theft and other irregularities (Vanasco, 1998).

Fraud is a pervasive fact of life in the business world (Luowers, et al., 2011). An auditor’s definition of fraud may be the following: The deliberate actions of a person or persons to mislead for the purpose of financial gain (Elder, et. al., 2010). Fraud is deliberate steps by one or more individuals to deceive or mislead with the objective of misappropriating assets of a business, distorting an organisation’s apparent financial performance or strength, or otherwise obtaining an unfair advantage (Hemrai, 2004). Where fraud is perpetrated by breaching security arrangements, organisations are reluctant to admit the commission of fraud. Auditors are committed to maintaining confidentiality as to their clients’ affairs (Humphrey and Turley, 1993).

In light of the above discussion, fraud may be defined as intentional deception, cheating or stealing and can be committed against users such as investors, creditors, customers or government entities (Weirich and Reinstein, 2000). Statement on Auditing Standards (SAS) No. 82 identified two categories of fraud as fraudulent financial reporting and misappropriation of assets (Crawford, 2011). Fraudulent financial reporting (management fraud) is where management seeks to inflate reported profits or other assets by overstating assets and revenues or understating expenses and
liabilities in order to embellish the financial statements. Misappropriation of assets (employee fraud) is where employees steal money or other property from their employers (Hemraj, 2004; Riahi-Belkaoui, 2000). Various fraud schemes could include embezzlement, theft of company property and kickbacks.

Common Symptoms of Acts of Fraud

The auditor should be acutely aware of both the common types or acts of fraud and related symptoms of fraud. The type or act of fraud is what actually causes a loss for the victim. It is what the fraudster tries to conceal. A symptom of fraud is a signal of fraud. However, the presence of a symptom does not necessarily mean that fraud exists (Hassink, 2010). The existence of a signal is a call for an inquiry and possibly an investigation. Statement of International Auditing Standards (SISAs) should be followed when fraud is suspected. However, the message here is that the auditor is obligated to be alert for the possibility of fraud (Hillison, 1999). After all, there are some general symptoms that sensitize the auditor to situations where fraud may exist as such (Lakshman, 2009):

1. Out of balance condition between a control account and its related chart of accounts.
2. Writing off receivables as bad debts and stealing the cash received on the accounts written off.
3. Differences reported by customers.
4. Collusion between buyer and seller to process refunds for goods not returned
5. Less responses to confirmation requests received than predicted.
6. Billing stolen merchandise to fictitious accounts.
7. Transactions do not have proper documentation.
8. Manipulating payroll records to divert wages, payroll taxes, or paycheques.
9. Suspicious year-end transactions.
10. Overstating hours worked or working unauthorized overtime.
11. Transactions posted without management's specific authorization.
12. Overloading expense accounts or diverting advances to personal use.
13. Failure to correct serious weaknesses in internal control.
14. Underpaying dividends to certain investors and diverting the difference to personal use.
15. Expense accounts in use with less than desirable controls in place.
16. Paying false invoices obtained through collusion with suppliers.
17. Unclear or evasive replies to audit questions.
18. Tasks assigned to employee that do not fit job description.

In addition to these, the auditor should be alert to situations in which there is (Sun, et al., 2006):

a) An incentive for gain. This may be direct (for example, a diversion of corporate assets) or in-direct (for example, increased compensation because of apparently profitable corporate performance).

b) Complex corporate structures and transactions. When such an incentive is present together with an artificially complex corporate structure, the auditor should become seriously concerned. Add to this a management dominated by one or a few individuals, an accounting department that is inadequately supervised and staffed, and operating on a crisis basis in the absence of control elements such as an internal audit group. Hence, the stage is set for fraud.

c) Related-party transactions. The matter of unusual or complex transactions lead the auditor to the related-parties area. A related party may be considered to be a company that is under common control with reporting entity, or under some circumstances, one that controls or is controlled by another related party. Examples of fraud, a common white-collar crime, are almost too numerous to list, but include: forgery, check kiting, lapping, kickbacks, computer fraud, bribery, payoffs, credit card fraud, defalcations, payroll padding, conspiracy, extortions, false entries, false advertising, price-fixing, and embezzlement (Hoi, et al., 2009; Churyk, et al., 2008).

Key Characteristics of Fraud Perpetrators and Motivations

Who is likely to commit fraud? Studies show that most corporate officers and other employees in positions of responsibility in accounting and data processing are most likely to commit fraud. Typically it is their appearance of sincerity and honesty which others tend to trust (Kranacher and Stern, 2004).
Beasley (1996) once highlighted that a man cannot be classified as honest or dishonest. He goes along with the game of life and can stand certain pressure for the sake of his ideals. But at a certain point he can stand no more. While this varies from one person to another, there seems to be a common denominator and that is that most embezzlers get involved with this activity as a result of financial need which is severe and which cannot be shared (Arens, et al., 2003). Once the opportunity for fraud has been ascertained and rationalized as a temporary borrowing, the embezzler is ready to put his plan in motion. He usually plans to repay what he has stolen. It is a surprising fact that in a large number of embezzling cases, a great deal of the money had been repaid and the culprits were discovered or caught before all the funds had been repaid (Arens, et al., 2003; Beasley, 1996).

It is important to note that a key factor in determining whether an individual will attempt fraud is the degree of control exercised by the company (Uzun, et al., 2004). In general, a person with a high level of personal integrity and limited opportunity or pressure to commit fraud will most likely behave honestly. But fraud becomes increasingly likely as individuals with less personal integrity are placed in situations where there are increasing pressures and greater opportunities to commit fraud (Erickson, et al., 2008).

**HOW FRAUD CAN BE PREVENTED IN COMPUTER TECHNOLOGY**

It was indicated by Fama and Jensen (1983) that anywhere from hundreds of millions of dollars to several billions are embezzled each year from U.S. corporations. Increasingly computers have been involved either directly or indirectly in such fraud (Erickson, et al., 2008). Dhillon (1999) also added that computer related fraud caused a lot of losses in organisations and it could be avoided if a more serious approach about the prevention and deterrence procedures was taken. Business and organisations were trying to cope with the intricacy and mystique that surrounds computer system. In addition, Haugen and Selin (1999) claimed that computer fraud was more perilous to organisations today. Furthermore, they elaborated on the common computer frauds, techniques used to commit fraud, the computer-based controls, as well as on how business assets can be protected. They stated that none of the organisations in the world could be 100 percent free of risk, and assessing an organisation’s risk to fraud was not easy. However, the risk could be mitigated by implementing a proper internal control system with good employment practices.

Moreover, during the last ten years no one argues that computers are "fraud-proof" as some did two decades ago, but there is still much disagreement as to what comprises computer fraud, where it begins, and how to prevent it (Seetharaman, et al., 2004). As a result of developing computer technology, the activities of accountants and auditors must indicate an understanding of computers so that computer security systems do not lack direction and focus. For more than two decades, computers were just coming into their own in the business world, and transactions could be traced manually. Colored ink and a basic knowledge of double-entry bookkeeping were the auditor's stock in trade at this time. Fraud was easier to perpetrate but also easier to discover (Desai, et al., 2006).

During the period of 1980s, many computer-assisted embezzlements are quite simple both in concept and in execution (Seetharaman, et al., 2004). One bank programmer simply raised his own overdraft limit by three digits (to $200,000) and lived in splendor until he was finally discovered. Another bank programmer instructed the computer to ignore any of his own personal checks whenever he had insufficient funds in his account to cover the check. He was caught by an ordinary clerk when the computer broke down one day and forced the bank to go back to processing checks by hand temporarily. EDP (electronic data processing) operator pushed the 'repeat' button on the printer to produce 200 extra copies of his own paycheck (Wright, 2000; Johnson, 1979).

A frequently used ploy involves instructing the computer to accumulate 'rounddowns' in the programmer's own personal account (Leahy, 2009). For instance, in one of the smoothest operations, a depositor removed blank counter deposit slips from a bank branch and replaced them with magnetic ink character recognition (MICR) encoded deposit slips from an account he had opened for himself. Four days later he withdrew $100,000 he had accumulated from other people's deposits and disappeared (Johnson, 1979).

Following are a number of possible explanations, according to (Hemraj, 2004), suggested as to why it is often easier to embezzle under a computerized system than under a manual system: With a computerized system, processing steps are decreased to a small number of computer programs. In a manual system, individuals have some control as
documents pass through the various accounting stages. Therefore, one computer programmer replaces a large number of accounting clerks. As a result, a dishonest programmer can create a large embezzlement scheme with more ease than any single accounting clerk it. In addition to this, records are ‘invisible’ in a computerized system; being magnetized bits on magnetic tapes, disks, or drums (Seetharaman, et al., 2004; Johnson, 1979). In a manual system, however, managers and auditors have ready access to visible ledger accounts (Hemraj, 2004).

Computers can be programmed to print out only certain items (the use of a management by exception format for reports is an example of this), with one result being fewer printouts (Range and Patterson, 2009; AICPA, 1985). Controls can be stored inside computer programs. For example, computers house edit routines to detect math errors or invalid transactions. This transfers the review function from people to the computer itself. However, this presents a potentially dangerous situation in that such controls are also invisible being stored inside the computer's memory, and can be changed by the programmer, through a program patch, for instance, to prevent their use in editing certain specified transactions (Erickson et al., 2008). Further, the internal control system has the same objective in both computerized and manual systems: to provide reasonable, but not absolute, assurance that the assets are safeguarded and the financial records are reliable (Desai, et al., 2006).

AICPA (1985) and Moscove (1978) offer a number of possible explanations for the absence of controls in the early years of computer technology. For example, in the beginning computerized systems were developed in such a haphazard fashion that people were content if their programs worked at all; they were not concerned about the possibility of a loss of security (Haugen and Selin, 1999). A pervasive ignorance of the finer points of computers on the part of executives lead to their subsequent abdication of responsibility of system security to the EDP managers (Chen, et al., 2006).

Many executives feel that because computer programs are often complicated, they are difficult to manipulate (Desai, et al., 2006). Many executives ignore the possible problems because the EDP system is not allocated a large portion of the company budget. EDP expenditures usually total less than one percent of revenues in. It is untrue that a company's potential losses from breaches of a computer system security are limited to the amount of the company's EDP-related expenditures. Many executives are in error if they feel that auditors protect them. Few auditors have the specialized knowledge of computer systems similar to a skilled computer programmer (Wright, 2000; Johnson, 1979).

Erickson, et al., (2008) and Arfield (1988) indicated that many executives believe that computer fraud is a rare occurrence. However, this is incorrect as companies absorb the loss in approximately 85 percent of those computer crimes that are detected to avoid public embarrassment and loss of confidence. On the other hand, they believe that computer technology allows new crime opportunities. There is more anonymity, less social control, and an electronic money market. Anonymity is increased through the development of data communications opening up opportunities for committing unlawful acts away from the scene of the crime (Desai, et al., 2006). Unfortunately, there is a dearth of controls for modern computer technology since the latest systems need different kinds of controls from those of the old manual systems. Consequently, this is the greatest weakness in the computer control structure (Hemraj, 2004; Arfield, 1988). Therefore, much attention has been given to improving techniques for auditing computerized information systems. For instance, a number of different checklists of questions and items to be examined are available to auditors to ensure the thoroughness of their audit of a computerized operation (Dhillon, 1999).

In the light of the above discussion, one such checklist is the SAFE (Security Audit and Field Evaluation for Computer Facilities and Information Systems) checklist which probes the following nine areas: 1) ‘personnel policies’ (who control data processing systems, or manage, operate, design, program), 2) ‘hardware controls’ (these may include the central processing unit, card reader, tape drives, disk devices, printers, terminals, and other devices), 3) ‘software controls’ (system programs and application programs), 4) ‘operating procedures’, 5) ‘backup provisions’, 6) ‘documentation’ (a description of system and its controls in relation to input, output, data processing, logic and operator instructions), 7) ‘insurance coverage’, 8) ‘security arrangements’, and 9) other supplemental areas of investigation (Uzun, et al., 2004; Hillison, 1999; Robertson and Frederick, 1988). During the auditor's examination, an auditor will check the operator's log, the security procedure violation log, the quality control reports, and the records of the input/output control section. The auditor could use manual techniques by auditing 'around the computer', relying on user controls and verifying output by its relationship to input (Kranacher and Stern, 2004). As with traditional
examinations, the auditor will also use sampling techniques to test for procedural weakness by determining the audit objective, defining the population, determining the sample size and evaluating the evidence (Erickson, et al., 2008). As with any audit, the auditor must be aware that there are certain limitations to testing. Testing records may not detect a fraud, even if it exists. This is especially so when collusion is involved (Hemraj, 2004). Thus, the auditor will choose certain transactions and follow them through the system to the final reports. Further, the auditor can test both the system’s validation controls and the security procedures by entering false transactions or by trying security violations.

METHODS OF COMPUTER SECURITY TO REDUCE FRAUD

Computer security can be improved by limiting access to the computer room. This approach involves improvements in physical security (Briney, 2000). For instance, one may limit the number of entrance and exit points to one each, with a system of positive identification. Such an approach would screen out outsiders, and screen out recently discharged employees. Though this may seem to be of little use, there have been a number of instances where disgruntled employees have damaged computer files when dismissed (Briney, 2000; Arfield, 1988). In addition to improving its control over access to the computer room, an organization can improve computer security by restricting access to the computer itself. However, companies must stress the importance of the basic principles of protecting the security of valuable assets, and make certain that all employees know of this enhanced security (Desai, et al., 2006; Elliott and Jacobson, 1987). For instance, controls should be established to ensure that only authorized users can ‘log on’ to the system and that they have access only to those parts of the system that they are authorized to use. This system is the one which is most commonly used; unfortunately, the more frequently it is used, the more likely it is to lose its security value. Here each person ‘logs on’ to the computer and has access to those files that management wishes him or her to have (Erickson, et al., 2008).

The password approach does not provide complete security. However, a number of procedural refinements have been developed to reduce the vulnerability of password systems (Dhillon, 1999); for example, the system should limit the number of attempts at access permitted from an on-line source or the amount of time permitted for responding correctly to the log-on sequence is limited to 30 seconds or thereabouts and is set to automatically shut off after two consecutive unsuccessful attempts. These steps would reduce the chance for attempting to penetrate the system through the ‘trial and error’ approach (Briney, 2000; Carrol, 1987; Sanders, 1985). Furthermore, it has been recommended that in order to keep a record of all unsuccessful attempts to break into a system, the computer must be programmed to keep a record of all such attempts. Currently, it has been suggested that access to unauthorized files be a more complicated operation. For instance, similar passwords might be changed on a regular basis and combined with information of a personal nature about the authorized user (Briney, 2000; Dhillon, 1999).

Ernst & Young (2002) stated that alternative methods to passwords also have been employed to control computer system access. One such method involves the use of magnetically encoded cards. For example, data encryption techniques for coding and decoding messages can be implemented on silicon chips in stations and host computers (Carrol, 1987). When authorized users access or send sensitive data, host computers generate random session keys to be used only for that exchange. Such a system ensures only that the card is correct, rather than that the person inserting the card is an authorized user of the card. There remains the possibility that cards can be illegally duplicated. However, a system that combines a card feature and a password feature might increase security (Chen, et al, 2006; Sanders, 1985; Carrol, 1987).

Other approaches that have been used include the matching of signatures, the matching of voiceprints, and the matching of hand geometry. In signature matching, the problem exists that the need to allow for a certain amount of variation in signature also permits the occasional acceptance of a good forgery (Briney, 2000; Arfield, 1988). Likewise, under a voice print-matching system a chance of error occurs from the need to allow for variations in voice inflection due to illness or speed. Over all, the use of hand geometry for identification is highly accurate due to the fact that it is extremely rare for two persons to have hands of exactly the same shape (Erickson, et al., 2008; Arfield, 1988).

Zhao, et al., (2004) stated that because of increasing incidences of computer fraud, auditors can no longer consider them of concern to law enforcement agencies. The extreme difficulty of detecting computer crime and of even
acquiring sufficient evidence to prosecute make it readily apparent that the only valid defense against computer crime lies in prevention (Seetharaman, et al., 2004). Protective measures cannot merely be addressed to the computer system itself. They must be implemented as a result of a complete rethinking of security strategy (Kranacher and Stern, 2004). Auditors must be alerted to the increasing occurrence of these crimes and should understand how to recognize them and how to inform management of ways to prevent them. Some of the computer-assisted embezzlements are elaborate while many are quite simple both in concept and execution (Zhao, et al., 2004).

Carrol (1987) indicated that crime by computer is categorized as indirect Fraud. This for example can be related to unauthorized use of a corporation's computer time by its computer personnel to process programs for people outside the company. Like the misuse of copying machines, the misappropriation of computer systems has probably victimized every corporation in this country (Wright, 2000). However, there have been several such cases of computer systems misappropriation which have been published revealing such blatant misuse that computer operators, were in effect, running a computer service bureau. Furthermore, the profit potential of such an operation can be dazzling - the employer unwittingly covers all the expenses (computer rental, labor, and supplies) and, in one case, was forced to upgrade his computer to meet the growing workload (Lakshman, 2009; Carrol, 1987; Johnson, 1979).

Crime by computer also is categorized as direct fraud. Even though fraud occurs through indirect use of computer, the most serious problems and largest financial losses happen when direct handling of the system is an essential part of the fraud plan. This direct handling could occur in several different ways (Wright, 2000; Carrol, 1987): a) managing the control of input data such as basic transactions, data adjustments, etc. b) the lack of well written computer programs or routines, or modifying to previously audited and approved programs without preauthorized action and c) the lack of control on creation of data files on magnetic tape or disk, i.e. master files.

Brandt R. Allen, Professor of Business Administration of the University of Virginia, attributes 73 percent of 40 billion dollar white-collar losses to transaction manipulation, including the alteration of documents. Professor Allen described the following situations (McArthur, 1981):

- A consultant to a West Coast bank circumvented internal controls in its money transfer area and stole $10.2 million. It was ten days before the bank even knew the money was gone.
- A teller supervisor changed computer records in a New York bank to permit him to steal over a million dollars without the bank finding out.
- A Chicago company disclosed a $12 million management fraud that was accomplished by computer manipulations. Professor Allen points out that one of the most difficult problems to overcome in precluding such fraud is the identification of improper transactions (Haugen and Selin, 1999). However, all of these methods have been used to defraud corporations.

**CONCLUSIONS AND CONTRIBUTIONS**

Fraud causes tremendous losses to the business world and creates morale problems in the workplace. These losses are serious problems to organisations that need to be managed, controlled and monitored. In this concern, the auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. Because of the nature of audit evidence and the characteristics of fraud, the auditor is able to obtain reasonable, but not absolute assurance that material misstatements are detected. Therefore, the role of the auditor is not to detect fraud, but in planning an audit so that there is reasonable expectation of discovery.

Auditors must always keep in mind that fraud is committed by top management may be more prevalent and harder to detect because an employee may be less likely to object if he is ordered to make false entries, and less likely to report his knowledge that the other person is doing so. In general, fraud detection is the responsibility of management, who controls the day-to-day running of the organisations. Auditors are not responsible for preventing and uncovering fraud. Auditors must do continuous risk assessment and tailoring of their audit strategy to suit. The attitude of professional skepticism also implies management must also be considered as a risk factor.
This paper has provided an overview of research on auditor’s responsibility to detect fraud on financial statements. It highlighted that a strong system of internal control is the most effective way of fraud prevention. Hence, the aim of this effort is to raise the level of security awareness for organisations in order to plan and facilitate a concerted effort to battle fraud, as prevention is better than cure. This paper also indicated that most accounting practitioners realize and acknowledge that auditors are often not positioned to detect the occurrence of fraud. Auditors lack the continuous presence necessary for the establishment and implementation of fraud prevention and deterrence programs.

There is always a possibility that an organisation’s financial statement may be distorted or misstated as the result of undetected fraud. The primary responsibility for the prevention or detection of fraud rests on management to develop adequate accounting system with appropriate internal controls. This does not mean that such a system will remove all risk of fraud; however, it will greatly reduce the risk of fraud. Therefore, the independent auditor must be aware that the possibility of fraud exists. The independent auditor’s primary concern is the fairness with which the financial statements present the financial position and operating results of the business entity.

The auditor can never be considered a guarantor of his client’s financial statements because of the fact that he maybe handicapped by collusion, expert forgery or other sophisticated deterrents to detection. However, he cannot avoid all responsibility for the detection of fraud, or his responsibility for conducting an adequate examination. The auditor’s primary responsibility is to his client. This responsibility is carried out primarily by following the generally accepted auditing standards. If the independent auditor fulfills his obligation under these standards, he cannot normally be held responsibility for undetected fraud. If, however, his negligence prevents his discovery of fraud and results in losses which could have been prevented by that discovery he may be held liable.

The auditor may assume that management is dishonest and is involved in fraud unless is an evidence to the contrary. He should not create conflict with management, but may provide advice and counsel to management in the preparation of financial information. This responsibility will assist in developing internal controls and procedures, and also may help to detect management fraud which is difficult to detect. In general, no one believes that people are more honest than they were many years ago. Also, the integrity of top management as a group is probably lower than it has been in the past. However, in my opinion, because of the use of advance and complex computer systems, the amount of fraud that is detected appears to have declined for several reasons, such as: systems are now more elaborated the changed role of the auditor, and different training of auditors. In general, the development of computer technologies in organisation has greatly enhanced the ability of people to defraud. The losses caused by fraud can only be estimated, as many cases go unreported or under reported. However, the overview of this research highlighted that the fraud losses incurred can be enormous.

Based on the previous conclusion, this study contributes to the knowledge that auditor must be aware of the possibility that fraud exists. It contributes to the knowledge and understanding of the nature of fraud and the auditor’s responsibility to detect material fraud. In general, auditor should look to improve the internal control systems and build an audit program which follows generally accepted auditing standards, which is maintained regularly to keep up with the changes in company operations. Also, the auditor should always check the input control first since that is the point at which transaction data is transferred and the risk of fraud highest. In this case, the auditor should look for authorized and approved inputs accept for processing by the computer center, where the audit procedures have been established. The paper also identifies the implications of frauds and errors which are material to the financial statement and may not be detected due to an oversight, but without negligence on the part of the auditors or management.

Overall, the overview from this paper showed a favourable picture on certain issues as auditor’s role may have attempted to portray the profession in a favourable light. Moreover, it would be interesting to investigating in future research the characteristics and general symptoms that sensitize the auditor to situations where fraud may exist. Thus, future research may consider sending a large-scale self-administered questionnaire to remove any potential bias. Further research into this area could also be undertaken to investigate the functional and operational aspects of auditing for fraud.
REFERENCES


Elder, J. R., Beasley S. M. and Arens A. A (2010), Auditing and Assurance Services, Person Education, New Jersey, USA.


Lakshman, N. (2009), Nine Charged in Hyderabad in Satyam Fraud”, Business Week, April 7th.
Leahy, J. (2009), Details of Alleged Satyam Fraud Emerge, January 22nd, Florida, USA.


McAthur, D. W (1981), Computer Fraud is Growing, Microfilm is one Solution, IMC Journal, 3rd quarter, pp. 21-22.


