International Journal of Economics, Business and Management Research

Vol. 2, No. 01; 2018

ISSN: 2456-7760

FRAUD PREVENTION IN PRIVATE SECTOR ORGANISATIONS

Abdul Baten*
Brentwood Open Learning College, United Kingdom

Abstract
In order to prevent fraud, detect fraud, or investigate fraud, one needs to understand fraud schemes as much as possible. The authors believe the best classification (taxonomy) for understanding fraud schemes is the one used by the Association of Certified Fraud Examiners (ACFE). There are several reasons for this choice. The ACFE is emerging as the primary antifraud organization. Its only purpose is the antifraud profession, whereas the American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA), and Information Systems Audit and Control Association (ISACA) have different primary objectives. Other groups have a similar goal, but none has the sole purpose of fighting fraud. As such, the ACFE's model serves as the de facto standard for the antifraud profession.

Keywords: Forecasting, Business Growth, Impact, Techniques, Market

Companies' boards of directors, management, and the public are asking why is fraud occurring and going undetected in our business systems. Auditors are asking themselves whether fraud can be detected when there is no predication or allegation of a specific fraud. Historically, the profession relied on evaluating the adequacy and effectiveness of internal controls to detect and deter fraud. Auditors would first document the system of internal controls. If internal controls were deemed adequate, the auditors would then test those controls to ensure they were operating as intended by management. The test of internal controls was based on testing a random, unbiased sample of transactions in the business system. In one sense, the search for fraud seems like a daunting responsibility. However, fraud in its simplest form should be easy to find. After all, the key to finding fraud is looking where fraud is and has been. This paper focuses on the use of fraud auditing to detect fraud in core business systems. Fraud auditing is a proactive audit approach designed to respond to the risk of fraud.

Identifying Fraud

Fraud and white collar crime have increased considerably over the recent years, and professionals believe this trend is likely to continue. The cost of fraud to businesses is difficult to estimate because not all fraud and abuse is discovered, not all uncovered fraud is reported, and civil or criminal action is not always pursued (Church et al, 2001). To discover fraud, you must know what fraud looks like. You must be able to identify symptoms in the data that point to fraud. The saying "it takes one to know one" does not mean that auditors and investigators need to commit fraud. However, if they wish to prevent fraud from happening, they must know who could be involved, what is possible, and how fraud could occur. Often the people who commit

* corresponding author +44 743785226, E-mail;

Vol. 2, No. 01; 2018

ISSN: 2456-7760

fraud are simply opportunists, taking advantage of a weakness or absence of control. Auditors must identify the opportunities before fraud takes place, and address any weaknesses in the controls if they hope to prevent fraud. But they also must be able to think like a perpetrator of fraud in order to detect the fraud.

One of the perpetual challenges that commonly introduces error into forensic analysis is evidence dynamics. Evidence dynamics is any influence that changes, relocates, obscures, or obliterates evidence, regardless of intent, between the time evidence is transferred and the time the case is adjudicated. It is because a piece of evidence can be related to a source in a number of ways. Identified control weaknesses must be examined from the point of view of who can benefit. Without a clear understanding of the control weakness, and an assessment of who could take advantage of the weakness, auditors are still somewhat in the dark. Assessing the degree to which people could benefit from the weakness gives you a measure of "opportunity." The fraud triangle—opportunity, rationalization, and pressure—is what drives people to commit fraud. The understanding of who could exploit the identified control weakness can focus the search for fraud on the persons with the greatest opportunity to commit the fraud.

Since fraud is often largely a crime of opportunity, control gaps and weaknesses must be found and, if possible, eliminated, or reduced. It is important to have a methodical approach to organizing and analyzing the large amounts of data that are typical when computers and networks are involved. Although the organizations implement good internal control, such control can deteriorate over time because of technological advances or human intervention. For example, Enron had effective internal controls and mostly correct financial reporting, but management overrode internal controls to create periodic and selective financial statement falsifications (Hurley and Boyd 2007). Thus, the management possibly overrode internal controls or the collusion existed between employees or third parties, such as vendors, clients, or politicians. Forensic science in general, and crime reconstruction specifically, provides such a methodology. Crime reconstruction is the process of gaining a more complete understanding of a crime using available evidence. We use evidence to sequence events, determine locations, establish direction or establish the time and duration of actions. Some of the clues that are utilized in these determinations are relational, that is, where an object is in relation to the other objects and how they interact or relate to each other. Other clues are functional, the way something works or how it was used, or temporal, things based on the passage of time.

Auditors must be aware of what can go wrong, how it can go wrong, and who could be involved. Individual behaviour is a product of an interaction between the person and the setting. . We have to accept that no business and no one is immune to fraud. A business, agency, or individual that thinks it is invulnerable to fraud is, in fact, the most inviting to fraudsters. It is important to note that while fraud does not occur randomly throughout an organization, neither does it occur in statistical proportions. Of course, there are areas of any business that are more vulnerable than others and the work environment is the key factor affecting the occurrence of fraud. Fraud, by its very nature, usually means that the activities are not easily uncovered or identified. Most criminological theory pays attention only to the first, asking why certain people might be more

Vol. 2, No. 01; 2018

ISSN: 2456-7760

criminally inclined or less so. This neglects the second, the important features of each setting that help to translate criminal inclinations into action

This preoccupation with criminal inclinations has produced a lop-sided picture of the causes of crime, but this is being corrected in new work by environmental criminologists, showing how some settings provide many more crime opportunities than others. Yet critics often downplay opportunities or temptations as true causes of crime. To show why this is mistaken we note that no crime can occur without the physical opportunities to carry it out. Whatever one's criminal inclinations, one cannot commit a crime without overcoming its physical requirements. Since crime opportunities are necessary conditions for crime to occur, this makes them causes in a strong sense of the word. At the same time, many people from uncaring or broken homes have never committed crimes, and many people from good families in comfortable circumstances have become active offenders. No theory about individuals can claim that it has found the necessary conditions for a person to commit crime. To be sure, no single cause of crime is sufficient to guarantee its occurrence; yet opportunity above all others is necessary and therefore has as much or more claim to being a "root cause".

In light of these and other events, critical areas of analysis, like fraud detection in the banking, insurance, and healthcare industries, must utilize better and more powerful systems to detect the anomalies and patterns contained in their data sources—that is, they must work smarter. Other areas of analysis, such as understanding consumer spending patterns, are becoming increasingly important as firms attempt to maximize revenues through targeted marketing and cross-selling while minimizing click fraud and other detriments to their operations. As companies become increasingly aware of their vulnerabilities, they look for new ways to identify, quantify, and protect themselves from the huge losses that fraud and security breaches can cause. Others want to stay abreast or ahead of their competition in the marketplace by managing their data more efficiently to identify improvements to their business processes and activities. All of these scenarios and situations are based on the ability to effectively access, integrate, and analyze data to expose new patterns.

Fraud Risk Assessment

To protect itself and its stakeholders effectively and efficiently from fraud, an organization should understand fraud risk and the specific risks that directly or indirectly apply to the organization. A structured fraud risk assessment, tailored to the organization's size, complexity, industry, and goals, should be performed and updated periodically (Maulidi, 2016a). The assessment may be integrated with an overall organizational risk assessment or performed as a stand-alone exercise, but should, at a minimum, include risk identification, risk likelihood and significance assessment, and risk response.

Fraud risk identification may include gathering external information from regulatory bodies (e.g., securities commissions), industry sources (e.g., law societies), key guidance setting groups (e.g., Cadbury, King Report 7, and The Committee of Sponsoring Organizations of the Treadway Commission (COSO)), and professional organizations (e.g., The Institute of Internal Auditors

Vol. 2, No. 01; 2018

ISSN: 2456-7760

(IIA), the American Institute of Certified Public Accountants (AICPA), the Association of Certified Fraud Examiners (ACFE), the Canadian Institute of Chartered Accountants (CICA), The CICA Alliance for Excellence in Investigative and Forensic Accounting, The Association of Certified Chartered Accountants (ACCA), and the International Federation of Accountants (IFAC). Internal sources for identifying fraud risks should include interviews and brainstorming with personnel representing a broad spectrum of activities within the organization, review of whistleblower complaints, and analytical procedures.

In 1987, the Treadway Commission reported, ``The potential of analytical review procedures for detecting fraudulent financial reporting has not been realized fully (National Commission on Fraudulent Financial Reporting [NCFFR], 1987)." Based upon a review of actual fraud cases, the Treadway Commission observed that financial statement frauds tend to be very similar in terms of how they are perpetrated. Most fraudulent cases involve improper revenue recognition, overstatement of assets, and/or improper deferral of expenses. Typically, analytical procedures involve comparing actual financial statement amounts with expected amounts that are derived from the application of a naive or complex prediction model. Since the misstatements resulting from fraudulent misrepresentations result in differences from predicted amounts, they should be potentially detectable with analytical procedures.

The central task of an auditor in applying analytical procedures is to develop expectations. The expectations the auditor develops will be based upon both the external information that the auditor encounters and his/her own existing knowledge stored in memory. An auditor's existing knowledge is an important factor in his/her understanding and interpretation of information, and can be expected to influence the auditor's effectiveness in assessing the risk of financial statement fraud. Extensive psychological research has investigated the existence and structure of knowledge utilized by decision makers, factors that influence the activation of the correct or most appropriate knowledge in a given decision-making context, and the impact of knowledge on the effectiveness and efficiency of decision-making processes. In addition, sensitivity analyses should be performed to determine the impact of the strength of evidence as a function of location in the network, and to investigate the effect of variability in the input strengths on the overall belief on each variable in the network.

From the technical standards of these three organizations, it is clear that auditors are expected to be able to identify key indicators of fraud in the process of performing professional services. Because of this fact, it is necessary for auditors to be trained in aspects of fraud identification and detection using red flags. It is also important for auditors to use training, articles, seminars, education, and other means to develop an effective mind-set related to fraud and especially to red flags. One more comment is necessary about technical standards and professional responsibilities. A study of red flags will enable auditors of all types to be able to recognize a red flag when it comes across their desks, and ends up under their noses, in daily activities. For example, would the auditor be able to recognize a red flag if he were doing the audit trail verification and picked up an invoice for a service that is printed using an Excel-generated format? Here are at least two red flags: Shell company schemes usually bill for a service, and

Vol. 2, No. 01; 2018

ISSN: 2456-7760

rarely do legitimate vendors use Excel as its billing system. This illustration could be told for countless other situations. But the bottom line is auditors need to have a high probability of recognizing an obvious red flag should they encounter one.

Managing the Business Risk of Fraud

As noted, fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain. Regardless of culture, ethnicity, religion, or other factors, certain individuals will be motivated to commit fraud. Organization stakeholders have clearly raised expectations for ethical organizational behaviour. Meanwhile, regulators worldwide have increased criminal penalties that can be levied against organizations and individuals who participate in committing fraud. Organizations should respond to such expectations. Effective governance processes are the foundation of fraud risk management. Lack of effective corporate governance seriously undermines any fraud risk management program. The organization's overall tone at the top sets the standard regarding its tolerance of fraud. The board of directors should ensure that its own governance practices set the tone for fraud risk management and that management implements policies that encourage ethical behaviour, including processes for employees, customers, vendors, and other third parties to report instances where those standards are not met. The board should also monitor the organization's fraud risk management effectiveness, which should be a regular item on its agenda. To this end, the board should appoint one executive-level member of management to be responsible for coordinating fraud risk management and reporting to the board on the topic.

Most organizations have some form of written policies and procedures to manage fraud risks. However, few have developed a concise summary of these activities and documents to help them communicate and evaluate their processes. An effective fraud risk identification process includes an assessment of the incentives, pressures, and opportunities to commit fraud. Employee incentive programs and the metrics on which they are based can provide a map to where fraud is most likely to occur. Fraud risk assessment should consider the potential override of controls by management as well as areas where controls are weak or there is a lack of segregation of duties. Assessing the likelihood and significance of each potential fraud risk is a subjective process that should consider not only monetary significance, but also significance to an organization's financial reporting, operations, and reputation, as well as legal and regulatory compliance requirements. An initial assessment of fraud risk should consider the inherent risk 8 of a particular fraud in the absence of any known controls that may address the risk.

Because financial statement fraud is typically committed by the top management team level rather than lower management or employees, one would expect incidences to occur most often in an environment characterized by irresponsible and ineffective corporate governance. Management would be more reluctant to engage in financial statement fraud when an effective corporate governance mechanism increases the probability of prevention and detection. Monitoring and oversight functions of corporate governance, including the board of directors and the audit committee, are thoroughly encouraged. Corporate governance refers to the way a

Vol. 2, No. 01; 2018

ISSN: 2456-7760

corporation is governed through proper accountability for managerial and financial performance. The characteristics and attributes of corporate governance most likely to be associated with financial statement fraud are aggressiveness, cohesiveness, loyalty, opportunism, trust, and control effectiveness. Aggressiveness and opportunism can be signified by the company's attitude and motivations toward beating analysts' forecasts about quarterly earnings or annual earnings per share and the attempt to make Wall Street happy by reporting unjustifiable favourable financial performance.

Cohesiveness and loyalty attributes create an environment that reduces the likelihood of whistle-blowing and increases the probability of coverup attempts. Trust and control ineffectiveness can cause those in an oversight function (e.g., board of directors, audit committee) as well as assurance function (e.g., internal auditors, external auditors) to be less effective in detecting fraud. The cohesiveness can cause a sharply defined group boundary of corporate governance that creates high cooperation among corporate governance members to conceal financial statement fraud and impose greater restriction of fraudulent financial information to leak to outsiders. This cohesiveness can encourage more collusion in the development of financial statement fraud, and if the fraud is discovered by internal or external auditors, push them for coverup. When the members of corporate governance establish trust, it creates less room for suspicion and scepticism, which in turn may reduce the likelihood of detection of fraud by auditors.

In addition, the board and senior management should communicate their commitment to fraud risk management. One method would be to embed this commitment in the organization's values or principles and code of conduct. Another method is issuing a short document (e.g., letter) made available to all employees, vendors, and customers. This summary document should stress the importance of fraud risk mitigation, acknowledge the organization's vulnerability to fraud, and establish the responsibility for each person within the organization to support fraud risk management. The letter should be endorsed or authored by a senior executive or board member, provided to employees as part of their orientation process, and reissued periodically. The letter could serve as the foundation for, and may be the executive summary of, a fraud control policy.

In summary, Logically, fraud is more likely to occur when there is strong motivation for financial gain, in other words, the perpetrator has a strong desire to obtain funds that are, in many cases, needed for very specific and compelling purposes. in order to combat fraud and white collar crime in businesses, a concerted effort must be exerted by the management of the business, the external auditors, and by all employees of the business. Everyone must realize that fraud is not a victimless crime. The cost of fraud and theft are shared by all through higher costs and lower corporate profits. A comprehensive strategy for fraud governance is essential if an organisation is to reduce the likelihood and impact of major fraud. Good fraud governance requires more than just ensuring an effective system of internal controls. It also requires a clear message and oversight from senior executives and non executives, clear policies and standards, knowledge of the key fraud risks, effective fraud reporting, fraud awareness training, and the development of a culture of high ethics and honesty (Maulidi, 2016b).

Vol. 2, No. 01; 2018

ISSN: 2456-7760

Forensic Soundness

As the field of digital forensics evolved from primarily dealing with hard drives to include any and all types of computer systems, one of the most fundamental challenges has been updating the generally accepted practices. There is an ongoing effort to balance the need to extract the most useful digital evidence as efficiently as possible, and the desire to acquire a pristine copy of all available data without altering anything in the process. In many situations involving new technology, particularly when dealing with volatile data in computer memory, mobile devices, and other embedded systems it is not feasible to extract valuable evidence without altering the original in some manner. Similarly, when dealing with digital evidence distributed across many computer systems, it may not be feasible to preserve everything.

In modern digital investigations, practitioners must deal with growing numbers of computer systems in a single investigation, particularly in criminal investigations of organized groups, electronic discovery of major corporations, and intrusion investigations of international scope. In such large-scale digital investigations, it is necessary to examine hundreds or thousands of computers as well as network-level logs for related evidence, making it infeasible to create forensic duplicates of every system. The purpose of a forensically sound authentication process is to support identification and authentication of evidence. In lay terms, this means that the evidence is what you claim and has not been altered or substituted since collection. Documentation is a crucial component of forensic soundness. Functionally, this process involves documenting unique characteristics of the evidence, like device IDs and MD5 hashes of acquired data, and showing continuous possession and control throughout its lifetime. Therefore, it is necessary not only to record details about the collection process, but also every time it is transported or transferred and who was responsible.

To cope with thousands, even millions, of transactions, and pick out the few that may be fraudulent, auditors and fraud investigators need powerful data analysis tools. However, the data analysis techniques that comprise state-of-the-art fraud detection tools can sometimes be perplexing. I hope that by shedding light on these techniques and providing easy-to-use fraud tests, Fraud Detection Techniques Using ACL will help auditors and fraud investigators discover fraud and take measures to prevent it. Most frauds are still discovered by outside sources such as police, anonymous letters, and customers. Others are discovered only by accident. This raises questions about the methods auditors are applying to seek out and investigate fraud. What's more, the amount of undetected fraud invites another question: Are auditors making effective use of data analysis software to detect fraud?. Identifying risks and measuring losses electronically can improve the overall quality of a fraud investigation. Results can help fraud investigators focus their efforts and address areas of abuse and fraud, rather than waste time reviewing valid transactions.

One of the most common forms of temporal analysis is creating a timeline to gain a clearer overview of events relating to a crime and to help investigators identify patterns and gaps, potentially leading to other sources of evidence. There are other approaches to analyzing

Vol. 2, No. 01; 2018

ISSN: 2456-7760

temporal data, such as plotting them in a histogram to find periods of highest activity. With great achievements come great responsibilities. Digital forensics has progressed rapidly but much more is required, including developing more sophisticated techniques for acquiring and analyzing digital evidence, increasing scientific rigor in our work, and professionalizing the field. This aims to contribute to the advancement of the field by expanding knowledge in the major specializations in digital forensics and improving our ability to locate and utilize digital evidence on computers, networks, and embedded systems.

Furthermore, this phase is sometime referred to as forensic examination, and involves verifying the integrity and authenticity of the evidence, performing a survey of all evidence to determine how to proceed most effectively, and doing some preprocessing to salvage deleted data, handle special files, filter out irrelevant data, and extract embedded metadata. This phase may include keyword searching to focus on certain items, and a preliminary review of system configuration and usage. This phase need not be limited to digital evidence, and can be augmented by interviews, witness statements, and other materials or intelligence. While forensic practitioners are gathering information about the crime under investigation, we develop possible explanations for what we are seeing in the digital evidence. Although such conjecture is often influenced by the knowledge and experience of a forensic practitioner, we must guard against preconceived notions that are based on personal prejudice rather than facts.

Various predictions will flow naturally from any hypothesis (if the hypothesis is true, then we would expect to find X in the evidence), and it is our job as forensic practitioners to determine whether such expectations are borne out by the evidence. The success of a forensic analysis hinges on how thoroughly an initial hypothesis is attacked. Therefore, it is crucial to consider other plausible explanations and include tests that attempt to disprove the hypothesis (if the hypothesis is false, then we would expect to find Y). If experiments and observations do not support the initial hypothesis, we revise our hypothesis and perform further tests. Once a likely explanation of events relating to a crime has been established, forensic practitioners must convey their work to decision makers. In summary, digital forensic analysis can play a direct role in identifying and apprehending offenders, helping investigators establish linkages between people and their online activities.

Assessing Alibis and Statements

Offenders and victims may mislead investigators intentionally or inadvertently, claiming that something occurred or that they were somewhere at a particular time. By cross-referencing such information with the digital traces left behind by a person's activities, digital evidence may be found to support or refute a statement or alibi. Investigators should not rely on one piece of digital evidence when examining an alibi—they should look for an associated cybertrail. On many computers it requires minimal skills to change the clock or the creation time of a file. Also, people can program a computer to perform an action, like sending an e-mail message, at a specific time. In many cases, scheduling events does not require any programming skill—it is a simple feature of the operating system. Similarly, IP addresses can be changed and concealed,

Vol. 2, No. 01; 2018

ISSN: 2456-7760

allowing individuals to pretend that they are connected to a network from another location. In addition, the location information associated with mobile telephones is not exact and does not place an individual at a specific place. As noted earlier, it can also be difficult to prove who was using the mobile telephone at a specific time, particularly when telephones or SIM cards are shared among members of a group or family.

The scientific method provides the final bulwark against incorrect conclusions. Simply trying to validate a theory increases the chance of error—the tendency is for the analysis to be skewed in favor of the hypothesis. This is why the most effective investigators suppress their personal biases and hunches, and seek evidence and perform experiments to disprove their working theory. Experimentation is actually a natural part of analyzing digital evidence. Given the variety and complexity of hardware and software, it is not feasible for a forensic analyst to know everything about every software and hardware configuration. As a result it is often necessary to perform controlled experiments to learn more about a given computer system or program. For instance, one approach is to pose the questions, "Was it possible to perform a given action using the subject computer, and if so, what evidence of this action is left behind on the system?" Suppositions about what digital evidence reveals in a particular case may be tested by restoring a duplicate copy of a subject system onto similar hardware, effectively creating a clone that can be operated to study the effects of various actions. Similarly, it may be necessary to perform experiments on a certain computer program to distinguish between actions that are automated by the program versus those performed by a user action.

Reference

Church, B. K., McMillan, J. J. & Schneider, A. (2001), 'Factors affecting internal auditors' consideration of fraudulent financial reporting during analytical procedures', Auditing: A Journal of Practice & Theory, Vol. 20, No. 1, pp. 65–80.

Hurley, D. A., & Boyd, D. (2007). Sarbanes-Oxley Act section 404: effective internal controls or overriding internal controls? *Forensic Examiner*, 16(2), 19–21.

Maulidi, Ach (2016a). Dealing with fraudulent financial statement in business organizations through whistleblowing system and staff awareness of fraud, *Proceedings of the International Conference on Accounting Studies* (ICAS), pp. 324-331. Published by Institute for Strategic and Sustainable Accounting Development (ISSAD), Universiti Utara Malaysia, UUM Sintok, Kedah, Malaysia.

Maulidi, Ach (2016b). Analyzing the worst corporate accounting scandals: theoretical framework perspective, Proceedings of the International Conference on Accounting Studies (ICAS), pp. 150-156. Published by Institute for Strategic and Sustainable Accounting Development (ISSAD), Universiti Utara Malaysia, UUM Sintok, Kedah, Malaysia.